平成 23 年度
内閣官房情報セキュリティセンター
委託調査

平成 23 年度

国民の情報セキュリティリテラシー向上に向けた検討

報告書

2012 年3月

株式会社 NTT データ経営研究所

1.　本調査・検討の概要

1.1. 本調査・検討の背景と目的

情報セキュリティに関する普及・啓発施策は、我が国における適切な情報セキュリティ水準を全体として確保・向上させるという観点、また国際社会での役割と責任の観点から、情報セキュリティ政策における特に重要な政策課題の1つである。

本検討は、情報セキュリティ普及・啓発プログラム[1]（2011 年7月8日情報セキュリティ政策会議決定)における「自己診断チェックリストの作成」および「高齢者向け資料の作成」について、情報セキュリティ2011[2]（2011 年7月8日情報セキュリティ政策会議決定)に基づき、現状や課題等についての調査、分析を行い、情報セキュリティに関する自己診断チェックリストや高齢者向け資料に盛り込むべき内容について明らかにするものである。

本検討では、昨今の情報セキュリティ情勢等を調査したうえで、各方面から具体的な課題を検討しつつ、有識者を交えた検討を受けて、国民の情報セキュリティリテラシー向上のため、情報セキュリティに関する自己診断チェックリストおよび高齢者向け資料に盛り込むべき具体的事項を抽出し、政府の資料作成の参考にすることを目的とする。

1.2. 委員会の開催概要

本調査・検討を進めるために委員会を組織し適宜検討をいただいた。

(1) 委員名簿

＜座長＞

今井　秀樹　中央大学　理工学研究所長

＜副座長＞

下村　正洋　株式会社　ディアイティ　代表取締役社長

＜委員＞

岡田　仁志　国立情報学研究所　情報社会相関研究系　准教授

小屋　晋吾　トレンドマイクロ株式会社　戦略企画室　統合政策担当部長

高橋　浩昭　株式会社　ビーシーキューブ　代表取締役社長

---

[1] 出典：http://www.nisc.go.jp/active/kihon/pdf/awareness2011.pdf

[2] 出典：http://www.nisc.go.jp/active/kihon/pdf/js2011.pdf

(2) 事務局

株式会社 NTT データ経営研究所

（統括責任者）

上瀬　剛　　ソーシャル・イノベーション・コンサルティング本部
アソシエイトパートナー

（実施責任者：プロジェクトリーダー）

松丸　剛　　情報戦略コンサルティング本部
シニアコンサルタント

（実施担当者）

秋元　祐紀　ソーシャル・イノベーション・コンサルティング本部
コンサルタント

2.　一般国民向け自己診断チェックリスト作成に向けた検討

2.1. 普及啓発対象者像

我が国では、インターネット利用者（以下、ユーザ）数が年々増加傾向にあるとともに、脅威のタイプが従来型に加えて複数を組み合わせた新たな攻撃が発生する情報セキュリティ情勢がうかがえるなか、ユーザは様々な不安を感じながらインターネットを利用している。

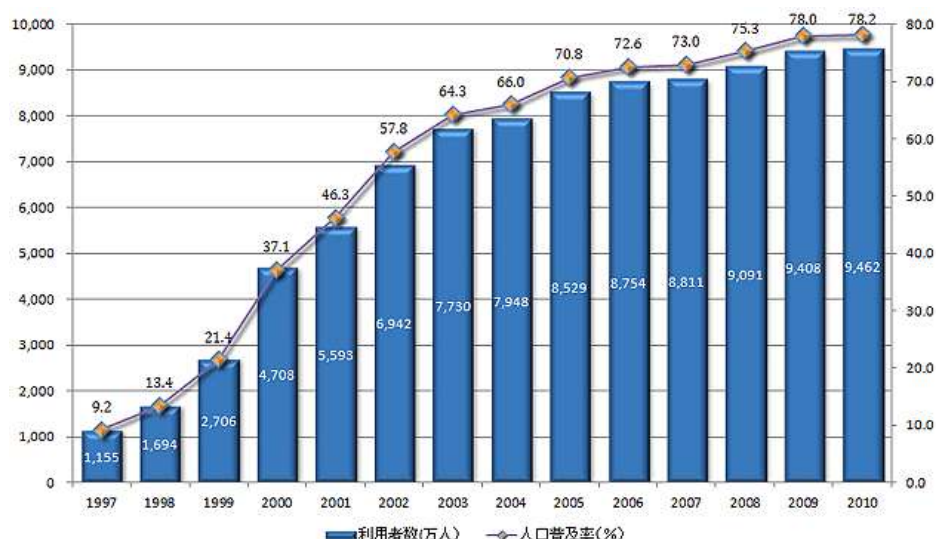
特に近年では、「どこまでセキュリティ対策を行えばよいか不明」、「セキュリティ脅威が難解で具体的に理解できない」、などの情報セキュリティに関する内容が正しく理解されていない傾向にある。

総務省が平成22年に実施した一般国民を対象とした情報セキュリティに関する脅威の認知度調査の結果から、一般国民は(A)情報セキュリティに関する脅威を認知していない人、(B)認知はしているが正しく理解できていない人、(C)認知しており、かつ正しく理解できていて行動に移せている人、の3つの層に大別できる。

本検討では、このような我が国におけるユーザの実態を踏まえて、情報セキュリティの普及・啓発を行う対象者像を、一般国民を情報セキュリティに関する知識の習得ステップの分類に従って、(A)と(B)の層とする。

本章では、まず情報セキュリティの現在の情勢および、ユーザの情報セキュリティリテラシーの実態を整理した後に、普及・啓発対象者像を明らかにする。

(1) 情報セキュリティ情勢

日本のユーザ数と人口普及率は年々増加傾向にある。例えば図表１にみるように、平成 22 年度には、インターネットを利用したことのある人は 9,462 万人、人口普及率は 78.2%と推計されている。

（注）

1. 平成 9～12 年末までの数値は「通信白書（現情報通信白書）」から抜粋。
2. インターネット利用者数（推計）は、6 歳以上で、調査対象年の 1 年間に、インターネットを利用したことがある者を対象として行った本調査の結果からの推計値。インターネット接続機器については、パソコン、携帯電話・PHS、携帯情報端末、ゲーム機等あらゆるものを含み（当該機器を所有しているか否かは問わない。）、利用目的等についても、個人的な利用、仕事上の利用、学校での利用等あらゆるものを含む。
3. 平成 13 年末以降のインターネット利用者数は、6 歳以上の推計人口（国勢調査結果および生命表等を用いて推計）に本調査で得られた 6 歳以上のインターネット利用率を乗じて算出
4. 調査対象年齢については、平成 11 年末まで 15～69 歳、平成 12 年末は 15～79 歳、平成 13 年末以降は 6 歳以上。

図表１　インターネット利用者数および人口普及率の推移[3]

[3] 出典：総務省「平成 22 年度通信動向調査」

また、図表 2 からインターネットの利用目的・用途としては、「電子メールの受発信」、「企業・政府等のホームページ（ウェブ）・ブログの閲覧」、「商品・サービスの購入・取引（デジタルコンテンツの購入および金融取引を除く）」、「個人のホームページ（ウェブ）・ブログの閲覧」、「デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の入手・聴取」が主なものとなっている。

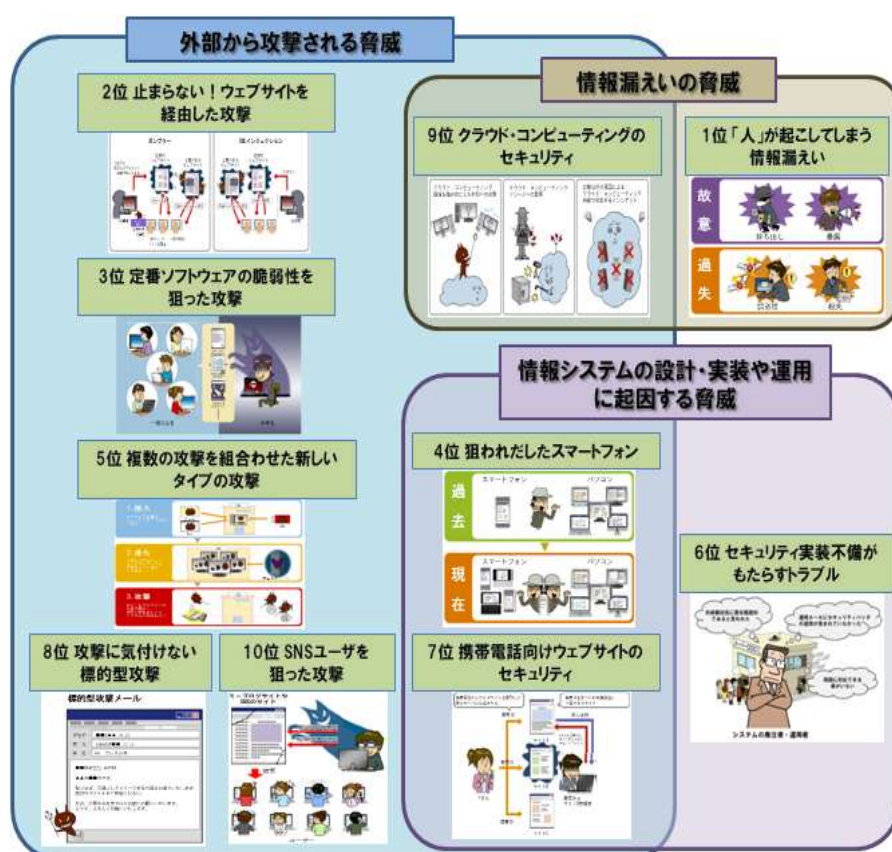
単位：%

		集計数（n）	1位	2位	3位	4位	5位
【全　体】		44,808	電子メールの受発信（メールマガジンは除く） 65.1	企業・政府等のホームページ（ウェブ）・ブログの閲覧 44.9	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 42.7	個人のホームページ（ウェブ）・ブログの閲覧 37.2	デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の入手・聴取 33.5
年齢階層	6～12歳	2,714	企業・政府等のホームページ（ウェブ）・ブログの閲覧 25.6	個人のホームページ（ウェブ）・ブログの閲覧 20.4	動画投稿サイトの利用 20.4	オンラインゲーム（ネットゲーム）への参加 17.3	デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の入手・聴取 14.3
	13～19歳	4,986	電子メールの受発信（メールマガジンは除く） 57.9	デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の入手・聴取 50.5	個人のホームページ（ウェブ）・ブログの閲覧 42.1	動画投稿サイトの利用 35.2	企業・政府等のホームページ（ウェブ）・ブログの閲覧 30.8
	20～29歳	6,382	電子メールの受発信（メールマガジンは除く） 76.3	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 55.4	デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の入手・聴取 55.0	個人のホームページ（ウェブ）・ブログの閲覧 47.7	企業・政府等のホームページ（ウェブ）・ブログの閲覧 45.7
	30～39歳	7,070	電子メールの受発信（メールマガジンは除く） 79.2	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 60.2	企業・政府等のホームページ（ウェブ）・ブログの閲覧 53.8	個人のホームページ（ウェブ）・ブログの閲覧 49.4	デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の入手・聴取 43.6
	40～49歳	7,766	電子メールの受発信（メールマガジンは除く） 75.7	企業・政府等のホームページ（ウェブ）・ブログの閲覧 56.8	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 52.8	個人のホームページ（ウェブ）・ブログの閲覧 40.9	地図情報提供サービス（有料・無料を問わない。乗換案内、ルート検索サービスも含む） 39.7
	50～59歳	7,926	電子メールの受発信（メールマガジンは除く） 65.9	企業・政府等のホームページ（ウェブ）・ブログの閲覧 50.0	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 40.3	地図情報提供サービス（有料・無料を問わない。乗換案内、ルート検索サービスも含む） 37.4	個人のホームページ（ウェブ）・ブログの閲覧 29.4
	60～64歳	3,481	電子メールの受発信（メールマガジンは除く） 62.4	企業・政府等のホームページ（ウェブ）・ブログの閲覧 42.3	地図情報提供サービス（有料・無料を問わない。乗換案内、ルート検索サービスも含む） 35.8	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 34.3	個人のホームページ（ウェブ）・ブログの閲覧 28.9
	65歳以上	4,483	電子メールの受発信（メールマガジンは除く） 42.1	企業・政府等のホームページ（ウェブ）・ブログの閲覧 26.0	地図情報提供サービス（有料・無料を問わない。乗換案内、ルート検索サービスも含む） 22.7	商品・サービスの購入・取引（デジタルコンテンツの購入及び金融取引を除く） 22.0	個人のホームページ（ウェブ）・ブログの閲覧 16.1

図表 2　年齢別インターネットの利用目的・用途（平成 22 年末）[4]

[4]出典：総務省「平成 22 年度通信利用動向調査」
http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201000_001.pdf

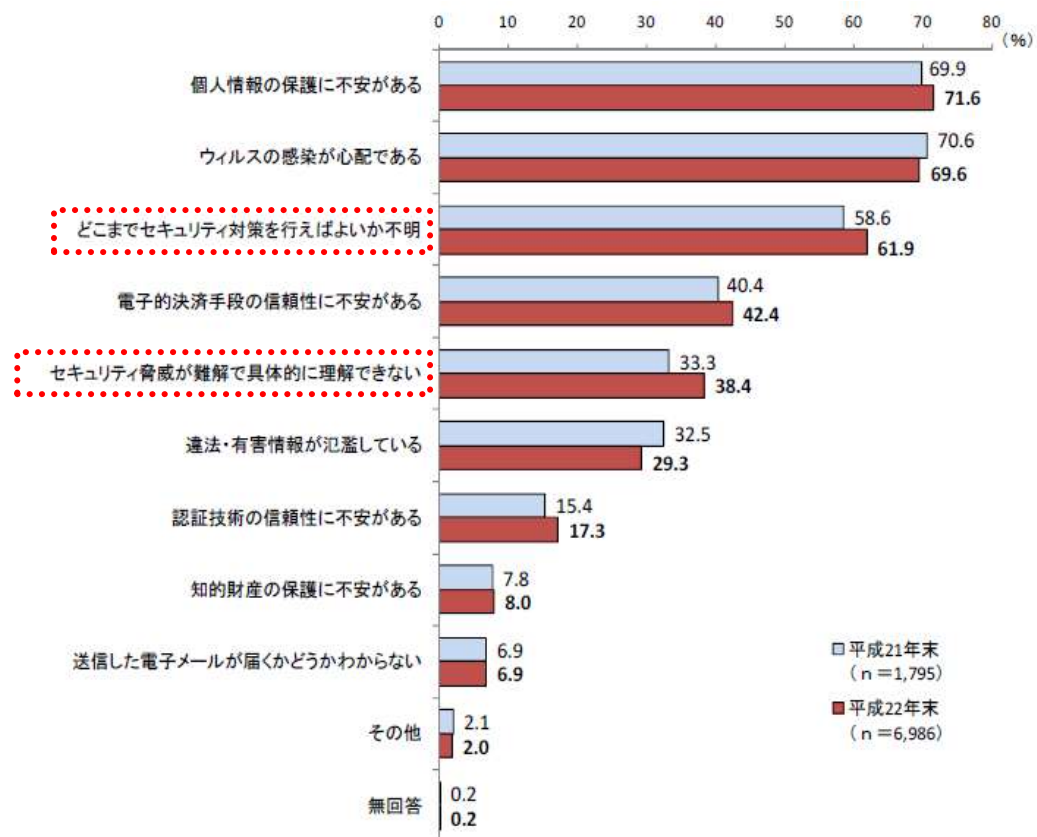
一方、近年の情報セキュリティを取り巻く状況[5]をみると、従来型のウェブサイト経由の攻撃や定番ソフトウェアの脆弱性を狙った攻撃に加えて、これら複数を組み合わせた新しいタイプの攻撃が発生してきている(図表3参照)。

また、攻撃もパソコンを対象としたものだけではなく、近年普及が加速しているスマートフォンユーザを狙ったコンピュータウイルスが出現するなど、新たな脅威が顕在化しつつある。

図表3　2011 年度版 10 大脅威[6]

攻撃手段としては、外部からの技術的な攻撃に加えて、標的型攻撃のように人間の心理的な隙や行動のミスに付け込んで個人がもつ情報を入手するなどの巧みなソーシャル・エンジニアリングの要素を併せ持つものも発生してきている。

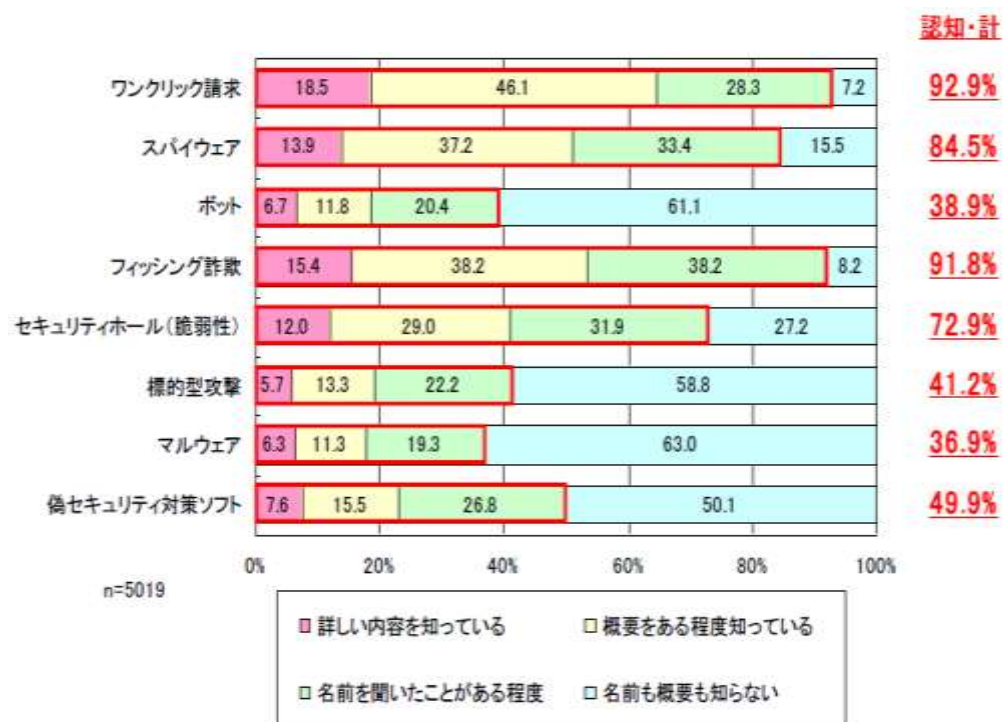
[5] 出典：独立行政法人情報処理推進機構 IPA「2011 年版 10 大脅威 進化する攻撃．．．その対策で十分ですか？」
[6] 同上

(2) インターネット利用時のユーザの心理状況

ユーザが年々増加するなか、図表 4 のインターネット利用時の心理面に目を向けると、情報セキュリティに対する不安が増加傾向にあることが分かる。例えば、平成 22 年度の総務省の調査では「どこまでセキュリティ対策を行えばよいか不明」のように、情報セキュリティ対策について理解はあるが対策の十分性がわからない人や、「セキュリティ脅威が難解で具体的に理解できない」のように、そもそも情報セキュリティに対する知識が乏しい人が増加している。

図表 4　インターネット利用で感じる心理状況[7]

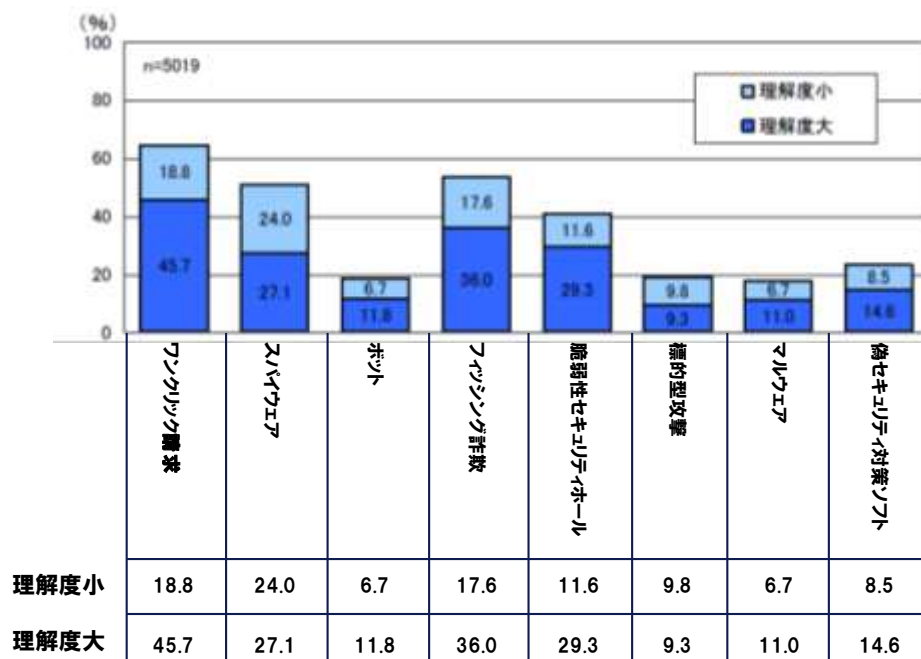
[7] 出典：総務省「平成 22 年度通信利用動向調査」

(3) 情報セキュリティに関する攻撃・脅威の認知度

情報セキュリティに関する攻撃・脅威の認知度に関する調査結果（図表 5）からは、ワンクリック詐欺やスパイウェア、フィッシング詐欺など、90%以上認知されている攻撃・脅威がある一方で、ボットやマルウェア、標的型攻撃は 40％程度と、認知度が低い項目が存在することが明らかになっている。

図表 5　情報セキュリティに関する攻撃・脅威の認知[8]

[8] 出典：独立行政法人情報処理推進機構 IPA「情報セキュリティの脅威に対する意識調査　報告書」2010 年 12 月

さらに、各脅威に関するユーザのリテラシーをみる（図表 6）と、90%以上認知されている攻撃・脅威について、正しく理解できている人は 50%未満である。脅威を用語として認知していても、正しい知識に基づいた理解ができていないことが分かる。

	ワンクリック請求	スパイウェア	ボット	フィッシング詐欺	脆弱性セキュリティホール	標的型攻撃	マルウエア	偽セキュリティ対策ソフト
理解度小	18.8	24.0	6.7	17.6	11.6	9.8	6.7	8.5
理解度大	45.7	27.1	11.8	36.0	29.3	9.3	11.0	14.6

※それぞれの情報セキュリティに関する攻撃・脅威について「詳しい内容を知っている」「概要をある程度知っている」と回答した人を対象とし、各攻撃・脅威の内容を問う設問において、全5問中4問以上正解の場合を「理解度大」、3問以下正解の場合を「理解度小」と定義している

図表 6　情報セキュリティに関する攻撃・脅威のリテラシー[9]

以上、我が国における情報セキュリティ情勢と国民のリテラシー実態を踏まえると、機能・サービスの多様化とともに従来型に加えて新たな攻撃手段が発生してきている。この環境下において、国民はその脅威を十分に認知していないだけでなく、認知していると感じている脅威についても内容を正確に理解できていない実態が明らかになった。

このため、国民の情報セキュリティリテラシー向上のためには、ユーザの利用環境においてどのような脅威があり、そこで自ら実施すべき対策は何なのかを各ユーザが知ることが必要である。

そこで、自身のやるべきことを理解するために、まずは自らが実施してい

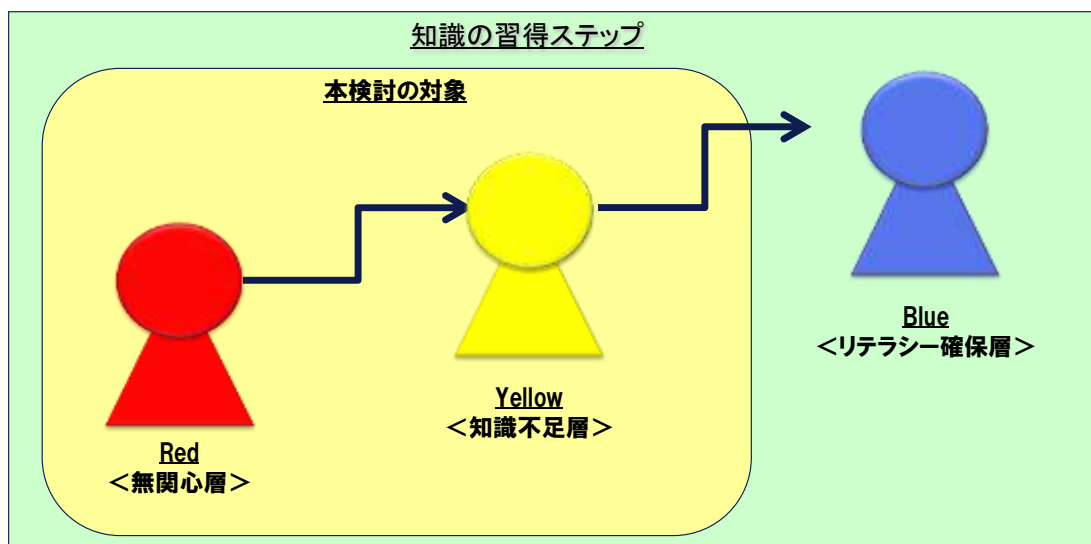
[9]出典：独立行政法人情報処理推進機構 IPA「情報セキュリティの脅威に対する意識調査　報告書」平成 2010 年 12 月

る対策がどのフェーズにあるのかを客観的に認識できることが取組みのスタート地点となる。そのためのツールとして、自己の情報セキュリティ対策の知識理解と実践が確認できる自己診断チェックリストの作成に関する検討を行う。

(4) 知識の習得ステップによる普及啓発対象者像

一般国民を対象にしていることから、普及啓発対象は、多様な整理が考えられ、性別、年齢、職業別など、分類軸は多岐にわたる。このようななか、本検討では、自らが実施している対策がどのフェーズにあるのかを客観的に認識できることを目的としているため、知識の習得ステップの考え方に着目して整理することとする。

知識の習得ステップは、情報セキュリティに関する脅威に対してそもそも認知していない人、認知しているが正しくは理解できていない人、正しく認知しておりかつ正しく行動できる人、の 3 つの段階で捉える。

本検討では、この 3 つの段階を信号が表現する 3 つのシグナルの考え方を用いて、ステップ 1 として“Red”、ステップ 2 として“Yellow”、ステップ 3 として“Blue”と名付ける。

図表 7　知識習得ステップによる普及啓発対象の分類

各分類は、以下のとおり定義する。

・Red：情報セキュリティに関心が低く、脅威を認知していないために情報セキュリティへの対策をとることができない、若しくはいい加減な対策をしている層（無関心層）。

・Yellow：情報セキュリティに関心があり、ある程度脅威及び対策を認知しているものの、その具体的取組みに関する理解度が十分でないため、正確な対策をとることができていない層（知識不足層）。

・Blue：情報セキュリティ対策を認知し、正しい対策をとっている層。
全ての国民が目指すゴールと位置付ける（リテラシー確保層）。

知識習得の3ステップは、情報セキュリティに関する認知度および理解度を向上させることで、危険信号である“Red”から“Yellow”“Blue”へと進展する。

本検討の普及啓発対象は、“Red”と“Yellow”とし、情報セキュリティに関する自己診断チェックリストの普及啓発（利用）を通じて、“Red”は“Yellow”へと、また“Yellow”は“Blue”へとステップアップすることを狙う。

2.2. 自己診断チェックリストの作成指針

本節では、はじめに普及啓発対象者ごとに提供する自己診断チェックリストの目的および各チェックリスト間の関係を整理したうえで、形式、内容について既存の取組み事例調査等を行い、そこから得られた知見等をまとめる。

その結果を受けて、「自己診断チェックリスト（赤版）」、「自己診断チェックリスト（黄版）」の作成指針を示す。

(1) 普及啓発対象者ごとに提供する自己診断チェックリストの目的と両リストの関係

①普及啓発対象者ごとに提供する自己診断チェックリストの目的

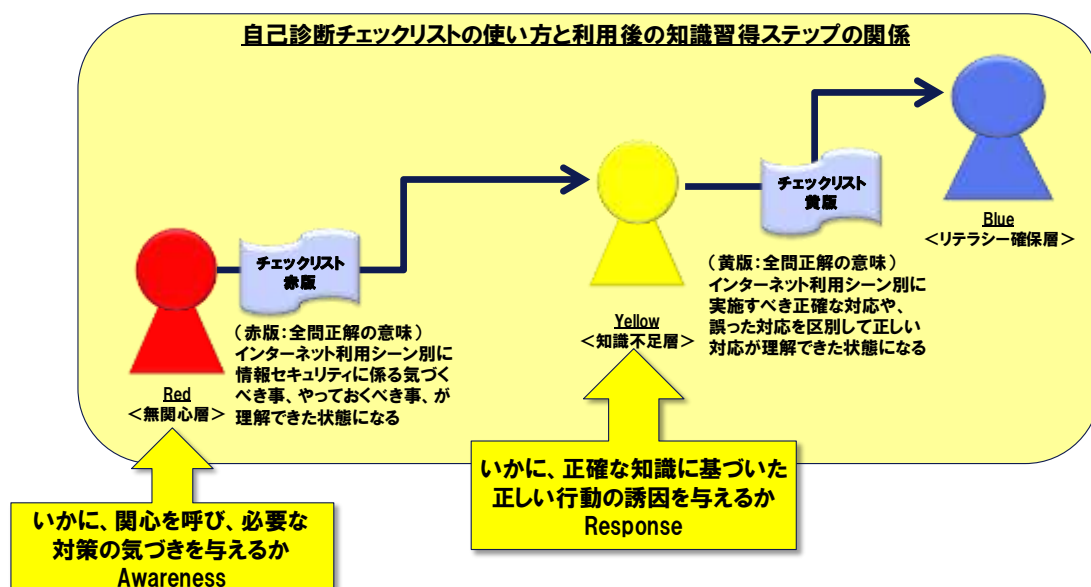
普及啓発対象者(“Red”と“Yellow”)は、情報セキュリティに対する関心度、理解度が異なるため、対象者ごとに普及啓発すべき事項も異なる。

“Red”は、無関心層であるため、情報セキュリティに対する関心を呼びおこし、必要な気付きを与えること(Awareness：アウェアネス)を目的とする。

一方“Yellow”は、知識不足層であるため、正確な知識に基づいた正しい行動の誘因を与えること(Response：レスポンス)を目的とする。

②両自己診断チェックリストの関係

両リストは、知識の習得ステップの各ステップ間をつなぐ役割をもつ。無関心層である“Red”は、「自己診断チェックリスト（赤版）」を全問正解することで、インターネット利用シーンごとに情報セキュリティに関心を持つことができ、気付くべき事項、やっておくべき事項を理解できた状態（“Yellow”）へとステップアップできる。

知識不足層である“Yellow”は、「自己診断チェックリスト（黄版）」を全問正解することで、インターネット利用シーン別に実施すべき正確な対応と誤った対応の違いを正しく理解できている状態にステップアップできる。この理解に基づいて日々行動することにより、“Blue”となることができる。

図表８　自己診断チェックリストの使い方と利用後の知識習得ステップの関係

(2) 自己診断チェックリストに盛り込むべき内容および形式

自己診断チェックリストに盛り込む事項としては、普及啓発対象者の目的に照らし合わせて、普及啓発内容としての記載事項（理解しやすい用語の使い方を含む)、記載事項をどのような様式（レイアウトを含む）でどの程度の記載ボリューム（分量）とするか等について、既存の取組み事例調査等を行い、そこから得られた知見等をまとめる。

①既存の取組み事例

自己診断チェックリストの内容・様式を検討するにあたって、情報セキュリティ分野にとらわれず、国内外の自己診断チェックリストに関する類似事例を調査した[10]。

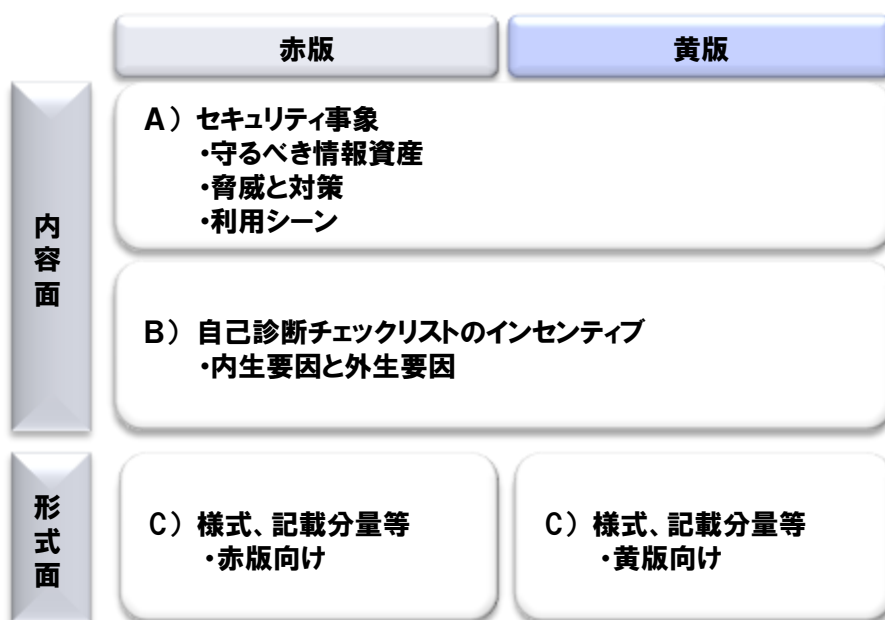
その結果、既存の事例からは、盛り込む内容および形式について、ベストプラクティスといえるようなガイドラインの存在は確認できなかった。そこで、国内の取組み事例のなかから、実際に取り組まれている組織・団体に対してインタビュー[11]を行った結果、各組織・団体は、自分たちの取組み目的に応じて、試行錯誤しながら形式を取りまとめていることが分かった。

また、用語の使い方については、テクニカルな内容に基づくものが散見され、自己診断チェックリストの利用者には理解が容易ではないものもあるという実態も確認できた。

[10] 調査結果は、「別添資料 5　国内事例集」、「別添資料 6　海外事例集」に取りまとめている。
[11] 東京都内の区役所、団体、等へ電話または訪問によるインタビューを行った。

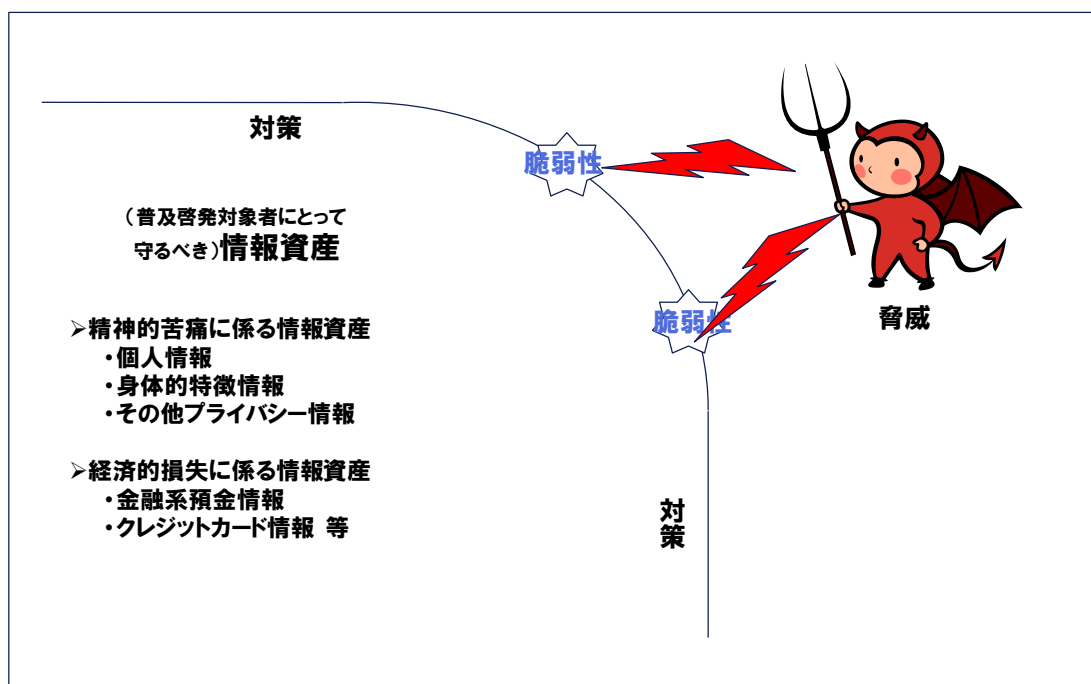
②内容および形式に関する検討結果

上記、既存の取組み事例の結果、自己診断チェックリストに盛り込むべき内容および形式がそのまま利用できるものを見出せなかったことから、自己診断チェックリストの目的に照らして、内容については、以下の 2 つの観点（　A）セキュリティ事象、B)自己診断チェックリストのインセンティブ　）から整理した。前者はどのような内容を記載するかであり、後者は記載文章の書き方の視点についての観点である。

形式については、各自己診断チェックリストごとに様式、記載分量をレイアウトも含めて整理（　C）様式、記載分量等　）した。

図表 9　自己診断チェックリストに盛り込む観点

A）情報セキュリティ事象

類似事例の取組みにおいて用いられているテクニカルな用語は、対象者が興味をもったり、理解するには適していないのではないか、という意見が検討委員の総意であった。このため、普及啓発の対象者が情報セキュリティリテラシーとして理解するに相応しい情報セキュリティ事象について、既存の事例に鑑み、解釈をしなおすこととした。

情報セキュリティ事象は、一般的に脅威と脆弱性とリスクの関係から整理すると、守るべき対象である「情報資産」、それを脅かす原因である「脅威」、それへの対策である「情報セキュリティ」の 3 要素で以下の図のように表せる。このような 3 要素がどのインターネットの利用場面（以下、利用シーン）で発生するか整理する。

図表 10　脅威と脆弱性とリスクの関係

本節では、国民の目線から、守るべき情報資産とは何か、情報資産を脅かす原因である脅威と実施すべき対策は何があるかをまとめたうえで、利用シーンごとに当てはめた。

A)-1　守るべき情報資産

本検討で扱う情報資産とは、企業における機密データではない。また、サーバーや通信装置でもない。あくまで、一般国民の視座に立った整理が求められる。

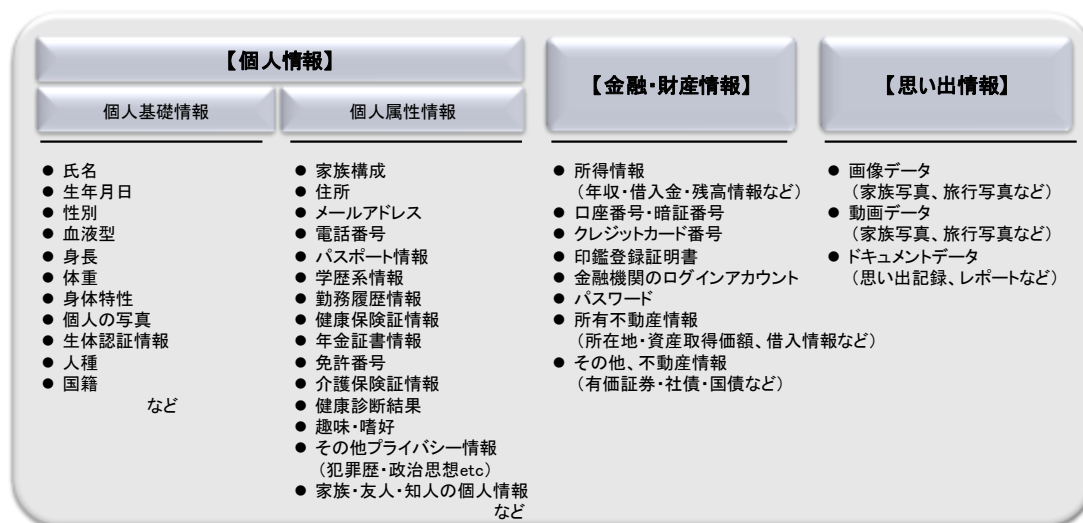
独立行政法人情報処理推進機構（以下、IPA）の調査結果によると、氏名やメールアドレスなどの個人情報の流出、デジタルカメラで撮影した写真データやWordで作成した文書の流出、クレジットカードの情報などの不正利用など、自分自身が所有している情報資産が被害にあうことに80%以上の個人が脅威を感じている。

本検討では、個人情報、思い出情報、金融・財産情報の 3 種類の情報を守るべき情報資産として扱う。

	脅威に感じる	やや脅威に感じる	どちらともいえない	あまり脅威に感じない	脅威に感じない
パソコンがウイルスに感染して氏名やメールアドレスなどの個人情報が流出してしまうこと	61.9	25.0	7.6	2.5	3.0
パソコン内に保存しているデジカメで撮った写真やWordで作成した文書などのデータが流出してしまうこと	51.7	28.7	11.5	4.6	3.6
代金を振り込んだのに商品が届かなかったり、クレジットカードが不正に利用されてしまうこと	69.8	17.6	7.9	1.8	2.9
お気に入りに登録したURLからアクセスしても、偽物のサイトに誘導させられてしまうこと	48.4	30.7	13.6	4.0	3.3
ウイルスに感染して、知らぬ間に他人のパソコンを攻撃してしまうこと	55.9	26.9	11.1	3.0	3.1
ウイルスに感染して、知らぬ間に他人宛にウイルスメールを送ってしまい、自分が犯人と誤解されてしまうこと	58.4	25.2	10.6	2.8	3.0

図表 11　情報セキュリティに関する攻撃の脅威度[12]

[12]出典：独立行政法人情報処理推進機構 IPA「情報セキュリティの脅威に対する意識調査　報告書」2010 年 12 月

各情報資産の具体例を図表 12 に示す。

図表 12　一般国民の視座に立った情報資産

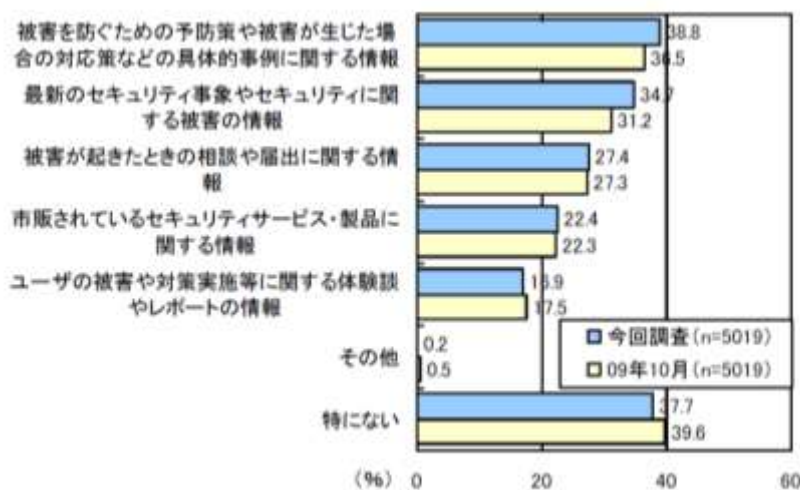
ここで留意すべきは、守るべき・守りたい情報資産には、自分自身の情報資産の観点だけでなく、第三者（家族や友人・知人等）の情報資産も含まれることである。さらに、そのような自分以外の者の情報資産を侵害しない、という面も考慮すべき点である。

近年、ブログ等を利用する際に友人や知人の情報資産を公開することは、個人情報保護の観点でプライバシーの権利に関わってくることが指摘されている。無意識に自分以外の人のプライバシーを侵害しているケースがあるので、その取り扱いには十分に注意する必要がある。例えば、思い出情報に属する画像データの場合、友人と 2 人で撮影した写真は友人のプライバシーに関わるので、インターネット上に公開する際には、友人に許可を得ることが必要になる。SNS（ソーシャル・ネットワーク・サービス）が普及したことで、インターネットを介して容易に写真や画像、その他多くの情報資産を共有できるようになり、他人の個人情報に対する情報セキュリティ意識の必要性が高まっている。自分自身が社会の一員として、守るべきものは何かを認識できることが重要である。

A)-2　脅威と対策

自分自身がどの脅威の被害にあったかを正しく認識し、適切な対策をとるためには、はじめに行動の背景・原因である脅威を整理する必要がある。

脅威はIPAの分類を参考に、「外部ネットワークや電子媒体を経由した脅威」「人的脅威」「アプリケーション等のセキュリティ対策や対応の不備に起因する脅威」の3観点に分類した。

対策は、IPAの調査（図表13）から、「被害を防ぐための予防や被害発生時対応策」、「被害発生後の問合せ先」であることが示されているため、「予防策」と発生後の被害を最小限に留める「事後対策」の2つに大別した。

図表13　一般国民が知りたいと思ったセキュリティ情報[13]

[13]出典：独立行政法人情報処理推進機構IPA「情報セキュリティの脅威に対する意識調査　報告書」2010年12月

本検討では、IPA の分類を参考とし、脅威は「外部ネットワークや電子媒体を経由した脅威」「人的脅威」「アプリケーション等のセキュリティ対策や対応の不備に起因する脅威」の 3 分類、対策は「予防策」と「事後対策」の 2 分類によって図表 14 に整理した。

脅威の分類	外部ネットワークや電子媒体を経由した脅威	人的脅威	アプリケーション等のセキュリティ対策や対応の不備に起因する脅威
脅威例	●技術的な脆弱性を狙った攻撃 ✓ 不正ｱｸｾｽ ✓ ﾏﾙｳｪｱ ✓ 標的型攻撃 ✓ SNSﾕｰｻﾞを狙った攻撃 ✓ ｶﾞﾝﾌﾞﾗｰ ✓ SQLｲﾝｼﾞｪｸｼｮﾝ ✓ APT攻撃 ✓ ｾﾞﾛﾃﾞｲ攻撃　など	●ヒューマンエラーに起因する脅威とソーシャルエンジニアリングに起因する脅威 ✓ 漏洩 ✓ 紛失 ✓ 盗難 ✓ 盗聴 ✓ うっかり　など	● 情報通信ｼｽﾃﾑの設計上の不備による問題 ✓ OS上の不備 ✓ ｱﾌﾟﾘｹｰｼｮﾝ上の不備 ✓ ﾈｯﾄﾜｰｸ上の不備 ✓ 利用サイト上の不備　など
予防策例示	● リスク軽減 ✓ ウィルス対策ソフトの導入・有効期間内での利用 ✓ 重要なデータはバックアップをする ✓ 有害なｳｪﾌﾞｻｲﾄへのｱｸｾｽを防止するｿﾌﾄまたはサービスの導入 ✓ パスワードの設定、更新、対策パッチあて ● リスク回避 ✓ 不要な電子ﾒｰﾙは開封しない ✓ 怪しいと思われるｳｪﾌﾞｻｲﾄにはアクセスしない ✓ セキュリティが促されたウェブサイトか見分け方を把握したうえで、利用時には確認する ✓ よく知らないｳｪﾌﾞｻｲﾄではﾌｧｲﾙをﾀﾞｳﾝﾛｰﾄﾞしない ✓ 安易に「はい」ボタンをクリックしない	● リスク軽減 ✓ 暗号化されたUSBﾒﾓﾘの利用や重要なファイルの暗号化 ✓ 通信（無線LANなど）の暗号化 ● リスク回避 ✓ 不要となった電子機器破棄、リサイクル時にはデータを消去する ✓ 他人に推測されにくいパスワードの設定及び定期的な変更 ✓ 家族と共有のパソコンを利用する場合の利用者ごとのログインアカウントおよびパスワードの設定及び適切な運用	開発、設計サイドの領域
事後対策例示	● インターネット回線をパソコンから抜く ● 不正請求等には、応じない、請求元に連絡しない ● システムの復旧/初期化を行う ● IPA等に報告する　など	● 警察に連絡する ● IPA等に報告する　など	

図表 14　情報セキュリティに関する攻撃の脅威と対策[14]

なお、図表 14 の整理は、国民が情報セキュリティリテラシーを取得した際に、実施すべき対策を示すことに着目している。アプリケーション等のセキュリティ対策や対応の不備に起因する脅威への対策は、情報通信機器[15]の開発・設計サイドの領域であるため、予防策等は対象外とした。

[14]出典：独立行政法人情報処理推進機構 IPA「2011 年度版 10 大脅威　進化する攻撃…その対策で十分ですか？」に基づき、NTT データ経営研究所にて編集・加工

[15] 情報通信機器とは、パソコン、携帯電話端末、スマートフォンなどのタブレット端末、等を含めて表現している。

A)-3　利用シーン

情報セキュリティリテラシーを向上させるためには、普及啓発対象者が関心を持って取り組めるように、自分がとるべき対策等を具体的にイメージしてもらうことが重要である。そのためには、ユーザの利用シーンごとに生じうる脅威と対策の具体例をまとめることが有効である。例えば、利用シーンとしてパソコン等を自宅から持ち出すシーンをイメージした場合、パソコン本体の紛失や盗難による情報資産の紛失や盗難などの被害が予想される。このような脅威への予防策として、パソコン本体に ID パスワードによるセキュリティロックをかけておくなどを挙げることができる。具体的な利用シーンの例を図表 15 に示す。

利用シーンは、時間軸で 1 から 5 を整理するとともに、「3. サービス利用時」は、「図表 2　年齢別インターネットの目的・用途」を網羅して整理した。

利用シーン	概要
1. 利用環境設定時	情報通信機器を購入後、利用出来るように設定するとき
2. 起動・立ち上げ時	スイッチを入れてサービスを利用できるように情報通信機器を立ち上げるとき
3. サービス利用時	情報通信機器を使用して、各種インターネット上のサービスを利用するとき
①企業・政府等のホームページ(ウェブ)・ブログの閲覧	企業・政府等のホームページ(ウェブ)・ブログの情報を(書き込みを行うことなく、単に)閲覧する(地図検索提供サービスの利用も含める)とき
②企業・個人等のホームページ(ウェブ)・ブログでの個人情報のやり取り(④を除く)	自身や家族・友人等の個人情報を入力して、企業・個人等のホームページ(ウェブ)・ブログを媒体に情報のやりとり(閲覧ではなく、)をするとき
③商品・サービスの購入・取引(⑤を除く)	ショッピング時における売買や金銭情報の入力などによりお金を扱うとき
④思い出情報(日記や各種記録)の作成・公開	思い出情報(日記や各種記録)を作成し、それらを情報通信機器上に保存したり、公開したりするとき
⑤デジタルコンテンツ(音楽・音声、映像、ゲームソフト等)の入手・聴取	自身の情報通信機器を利用して、デジタルコンテンツ(音楽・音声、映像、ゲームソフト等)の入手・聴取(動画投稿サイトの利用も含む)するとき
⑥ネットワークを介したゲームや家電機能の利用	オンラインゲーム(インターネットを介するゲーム)やネットワーク家電の機能を利用するとき
⑦自身のブログ等の作成	自身のブログなどのサービスを開始するために、自身の情報に関する設定作業を行うとき
⑧電子メール利用	電子メール機能を利用(送信・受信)するとき
4. 自宅外への持出時	情報通信機器(USBや個人情報を掲載した紙媒体を含む)を自宅外に持ち出すとき
	情報通信機器を自宅外に持出して利用するとき
5. 利用していない時	情報通信機器を利用していない状態のとき

図表 15　　利用シーン一覧表

A)-4　普及啓発の対象とする情報セキュリティ事象（まとめ）

上記 A)-1 から A)-3 までを踏まえて利用シーンを軸に図表 16 に一覧を整理する。

利用シーン	情報セキュリティ事象	赤版での取扱	黄版での取扱
1. 利用環境設定時	脅威：利用環境のセキュリティが設置されていない場合、各種攻撃、不正アクセス、不正利用の危険 対策：インターネット利用時のセキュリティツールの設置(ウイルス対策ソフトの導入、セキュリティパッチの適用、等)	➢1 ➢3	Q1、Q3、Q4
2. 起動・立ち上げ時	脅威：機器の起動時は自分以外の第三者に機器を自由に利用される危険 対策：機器起動時のログインID・パスワード設定、等	➢2	Q2
3. サービス利用時	－－－－		
① 企業・政府などのホームページ(ウェブ)・ブログの閲覧	脅威：OSやソフトウェアの脆弱性が修正されていない場合、不正アクセスやコンピュータウイルスなどの攻撃等 対策：セキュリティパッチの適用、ウイルス対策ソフトの更新、等	➢4	Q18
② 企業・個人などのホームページ(ウェブ)・ブログでの個人情報のやり取り(④を除く)	脅威：個人情報の侵害・漏えい、紛失 対策：個人が特定される情報を安易に公開しない(公開範囲の制限)、個人情報が保存されたファイルには、暗号化やパスワードを設定、バックアップ、等	➢4	Q5、Q6
③ 商品・サービスの購入・取引(⑤を除く)	脅威：金融・財産情報の漏えい、紛失、等 対策：ネットバンキング用のID・パスワードは類推されにくいものの設定、管理、ネットバンキング利用履歴の消去 金融機関を名乗りネットバンキング用のID・パスワードの入力を促すメールが届いても安易に教えない、等	➢7	Q7、Q8
④ 思い出情報(日記や各種記録)の作成公開時	脅威：プライバシーの侵害、等 対策：情報漏えいの可能性が伴うファイル共有ソフトを利用しない、インターネットに公開する写真や動画は、関係者に公開することの許可、公開時の情報取捨選択、バックアップ、等	➢4 ➢6	Q9、Q10、Q11
⑤ デジタルコンテンツ(音楽・音声、映像、ゲームソフトなど)の入手・聴取	脅威：ウイルス感染、等 対策：ウイルス対策ソフトの導入・パターンファイルの最新化、「ホームページの信頼性評価」を用いたサイトの利用	➢8	Q12、Q13
⑥ ネットワークを介したゲームや家電機能の利用	脅威：①から⑤と同様の脅威が想定 対策：①から⑤と同様の対策を想定	➢12	Q16、Q17
⑦ 自身のブログなどの作成	脅威：②から④と同様の脅威が想定 対策：②から④と同様の対策を想定	➢5	Q18、Q19
⑧ 電子メールの利用	脅威：電子メール受信時にはウイルス感染・成りすまし等の危険、送信時には誤送信・情報漏洩の危険 対策：身に覚えのないアドレスから届いたメールの添付ファイルは安易に開封しない、覚えのないアドレスから届いたメールには返信しない、電子メールを一括送信するときは、Bccで送付する	➢9	Q14、Q15
4. 自宅外への持出時	脅威：紛失・盗難 対策：貴重品を扱うように常に所在を意識した行動 USBの中のファイルにパスワードの設定、事前にデータバックアップ	➢10	Q20、Q21
5. 利用していない時(トラブル対応)	脅威：トラブル発生時には、どのように対応、どこへ連絡・相談してよいか分からない 対策：インターネットに有線で接続している場合、回線を抜く 一人で悩まず、誰かに相談する	➢11	Q22

図表 16　情報セキュリティ事象一覧

B)自己診断チェックリストのインセンティブ

普及啓発対象者に自己診断チェックリストを広く普及するためには、多くの普及啓発対象者が自己診断チェックリストに対して関心を持つことが重要である。そのためには、普及啓発対象者が自己診断チェックリストを実行するためのインセンティブを明確にする必要がある。「自己診断チェックリストに答えれば、あなたはどんな被害に遭遇するか理解できます」などは、インセンティブの一例である。

自己診断チェックリストの普及のためには、インセンティブとして内生要因（自分自身のため）と外生要因（家族や社会のため）の両面を備えることが重要である。広く一般国民に普及している取組み事例として、インフルエンザ予防策が挙げられる。インフルエンザ予防策では、個人を感染から守るという内生要因の他に、マスクを付けて集団感染を予防するという外生要因も働いている。他にも、交通安全運動や火の用心などの活動も内生要因、外生要因が両立した成功事例として挙げられる。

本検討では、内生要因（自分自身のため）と外生要因（家族や社会のため）、という観点から、興味を湧かせる表現方法を自己診断チェックリストの内容に反映させることとした。

図表 17　内生的、外生的インセンティブの例（インフルエンザ予防）[16]

[16]出典：厚生労働省　http://www1.pref.shimane.lg.jp/contents/kansen/inf/pdf/poster23.pdf

C)様式、記載分量等

「自己診断チェックリスト(赤版)」はアウェアネスが目的であることから、その形式は、事例調査結果及び有識者との検討会を踏まえ、以下のとおり整理した。

・分量が一目して把握できる簡潔な質問構成レイアウト（Yes/No 方式）であること
・質問文は、短く、回答しやすい内容であること
・取組み易さを考慮して、回答時間は短くなるよう配慮すること
・「情報セキュリティ対策の 10 カ条」のように、自身で取組み結果を整理しやすいよう考慮すること

「自己診断チェックリスト（黄版)」はレスポンスが目的であることから、その形式は、事例調査結果及び有識者との検討会を踏まえ、以下のとおりとした。

・通勤通学の電車内で取り組むことや、学校の授業での利用を想定した分量とすること
・質問形式は、回答しやすさの観点から択一方式であること
・質問文は、利用者の情報セキュリティ知識が一定でないことから、利用シーンにおける行動の正誤等を問う構造にすること
・全てじっくり読まないと判断できない選択肢ばかりでは、疲労によりチェックを途中でやめてしまうことも考えられるため、瞬時に排除できる項目やリラックスできるような項目内容を散りばめて設定すること

(3) 自己診断チェックリストの作成指針

自己診断チェックリスト（赤版）および自己診断チェックリスト（黄版）の作成指針は以下のとおりとする。

①自己診断チェックリスト（赤版）の作成指針

- ✓ 普及啓発目的 ・・・アウェアネス目的
- ✓ 形式（様式)・・・・セキュリティ対策事項 10 カ条のように「やるべき事」リストになる Yes/No 回答型
- ✓ 形式（記載分量)・・1 枚に設問・回答欄をまとめるよう記載分量を設定する
- ✓ 内容・ ・・・・・・利用シーンを網羅して、情報セキュリティ対策の予防、事後対応等を扱う内容とする。

「自己診断チェックリスト(赤版)」の対象者は､無関心層であることから、自身の情報セキュリティの取組み状況が、当チェックリストによって、一目で把握できるよう作成する。そのために、どの利用シーンで自分の取組みが出来ていて、どの利用シーンで出来ていないかを客観的に掴めるよう、設問は利用シーンごとにレイアウトする。

②自己診断チェックリスト（黄版）の作成指針

- ✓ 普及啓発目的 ・・・レスポンス目的
- ✓ 形式（様式)・・・・3 択型、解説は回答後に確認するレイアウト
- ✓ 形式（記載分量)・・通勤通学の電車内で取り組むことや、学校の授業での利用を想定した分量
- ✓ 内容 ・・・・・・・利用シーンを網羅して、情報セキュリティ対策の予防、事後対応等を扱う内容とする。

「自己診断チェックリスト（黄版)」の対象者は、知識不足層であることから、情報セキュリティに関する理解度が様々な層で構成されていることが推測される。本普及啓発対象者の共通概念は、利用シーンだけであることが想定できるため、設問は利用シーンを示し、回答には正しい対策を問う、または誤りの対策等を問う選択肢を設定する。取り組みやすさを考慮して、選択肢は必ず設問内容と文脈を整合させるとともに、明らかな誤りを入れるなどの配慮も行う。

2.3. 自己診断チェックリストの配布方法

情報セキュリティに関する自己診断チェックリストの配布は、既存の取組み事例調査等を行い、そこから得られた知見等をまとめて整理する。

(1) 自己診断チェックリスト配布方法の一般的な考え方

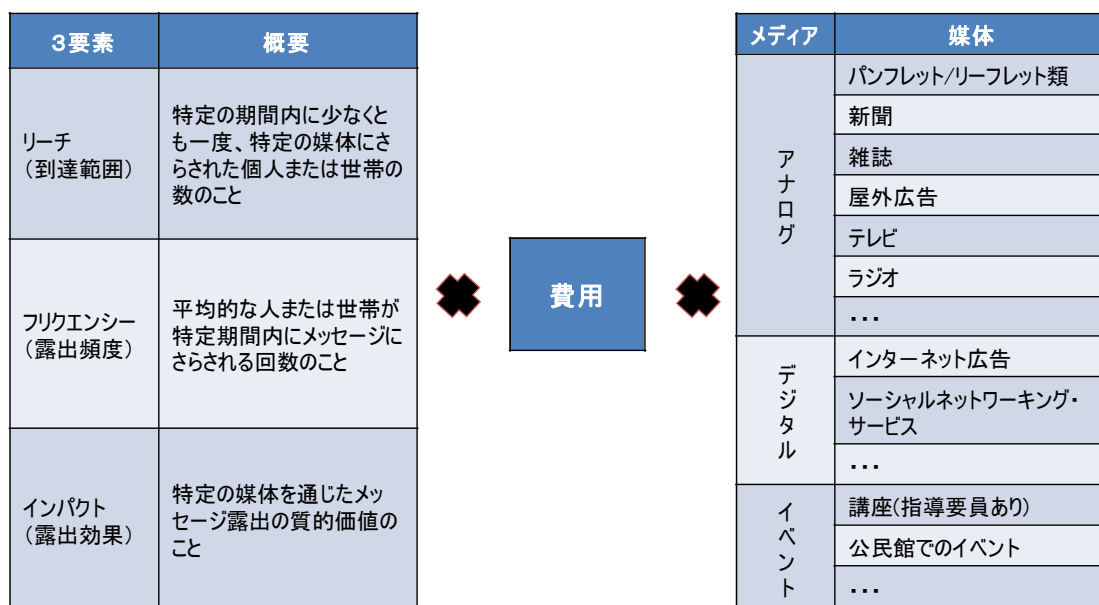
施策のメッセージを広く伝える配布方法を考える際には、まず媒体選択を考えるのが一般的である。媒体を選択の考え方は、普及啓発対象者に対する“リーチ(到達範囲)”、“フリクエンシー(露出頻度)”、“インパクト(露出効果)”の3つの要素から評価する[17]。

媒体選択とは、普及啓発対象者に理想的な頻度でメッセージを伝えるために、最も費用効果が高い媒体を見つけることである。リーチ、フリクエンシー、インパクトはいずれも投資すれば、効果を高めることができる。ただし、媒体を選択する際には、投資できる予算は限られていることを念頭におき、費用面も考慮に入れることが重要である。どこに投資するべきか、重点を置く領域とそうでない領域のバランスを考える必要がある。

媒体はそれぞれ個別の長所や短所を持つ。このため、上記3要素に応じて、適切な媒体を選択することになる。

3要素	概要
リーチ（到達範囲）	特定の期間内に少なくとも一度、特定の媒体にさらされた個人または世帯の数のこと
フリクエンシー（露出頻度）	平均的な人または世帯が特定期間内にメッセージにさらされる回数のこと
インパクト（露出効果）	特定の媒体を通じたメッセージ露出の質的価値のこと

✖ 費用 ✖

メディア	媒体
アナログ	パンフレット/リーフレット類
	新聞
	雑誌
	屋外広告
	テレビ
	ラジオ
	・・・
デジタル	インターネット広告
	ソーシャルネットワーキング・サービス
	・・・
イベント	講座(指導要員あり)
	公民館でのイベント
	・・・

図表 18　配布媒体選択の3要素

[17]出典：PEARSON　「コトラー&ケラーのマーケティング・マネジメント第12版」p714-717 2009年9月

一般的に選択対象となる媒体は、以下の図表 19 のようなメディア型とイベント開催型となる。メディア型とは、普及啓発対象者に情報を伝達する際の媒体にテレビやラジオ等の電波媒体や、新聞や雑誌などの紙媒体、またインターネット広告などの電子媒体といった、人が直接会わずとも情報を伝えることができるものである。一方、イベント開催型は、サポータや講師と呼ばれる人が直接対象者とコミュニケーションを取りながら情報を伝達するものである。

※1アナログメディア：インターネットを介さない伝達媒体
※2デジタルメディア：インターネットを介した伝達媒体

情報伝達媒体	メディア型			イベント開催型
	アナログメディア※1		デジタルメディア※2	イベント（人）
	マス向け媒体	ターゲット向け媒体		
媒体（例）	• テレビ • ラジオ • 新聞 • 雑誌 • 屋外看板 • ポスター • のぼり・幕 • チラシ • イエローページ • パンフレット	• 回覧板 • 手紙 （ダイレクトメッセージ）	• インターネット広告 • モバイル端末からの情報共有 • メール、メーリングリスト広告 • SNS • 電子看板	• 講座（指導要員必要） • 学校教育 （指導要員必要） • 表彰制度 • 親子イベント • 公民館イベント • 挨拶、ボランティア活動（ボランティア要員必要）
特徴	一般大衆に広く伝達することが可能であるが、一方向的にしか情報を伝達できない。デジタルメディアに比してコストがかかることがネックとなる。	ターゲットが絞られることで、対象と明確な目的を持って情報共有をすることができる。ただし、リーチできる範囲は限定される。	低コストで広範囲に情報を伝達することができる。双方向的に情報をやり取りすることができる。時間的、空間的制約が少ない。	人と直にコミュニケーションを図りながら情報を伝達できるのが特徴であり、他の手段に比して、情報の深く正確に相手に伝えることができる。ただし、活動範囲が限定され、また人件費が高いことがネックとなる。

図表 19　一般的な情報伝達媒体一覧

また、図表 20 に媒体の特徴を整理した。

メディア	媒体	長所	短所
アナログ	パンフレット/リーフレット類	柔軟性がある。完全に管理できる。メッセージを演出できる。	作りすぎ(数量)が無駄に繋がる。
	新聞	柔軟性がある。タイムリー、地元市場をよくカバーする。幅広い受容、高い信用度	短命。再生の質が悪い。回覧読者が少ない。
	雑誌	地理的、人口動態的に選択できる。高い信用度と信望。高い再生の質。寿命が長い。回覧読者が多い。	広告が出るまでのリードタイムが長い。無駄がある。掲載位置の保証がない。
	イエローページ	地域市場を隅々までカバーする。高い信用度。リーチが幅広い。低コスト。	競争が激しい。広告が出るまでのリードタイムが長い。クリエイティブ面で限界がある。
	屋外広告	柔軟性がある。繰り返し露出される。低コスト。競争が少ない。	対象の選択が困難。クリエイティブ面で限界がある。
	回覧板	対象の選択が容易。完全に管理できる。対話の機会がある。比較的低コスト。	コストがかさむ恐れあり。
	テレビ	映像・音・動きを統合。五感に訴える。高い注目度とリーチ。	極めて高コスト。雑多な広告が氾濫、露出が短い。対象の選択が困難。
	ラジオ	大衆に届く。地理的・人口動態的に選択できる。低コスト。	聴覚のみに訴える。テレビより注意を引きにくい。視聴者が一定でない。露出が短い。
デジタル	インターネット広告	対象を選択できる。対話の機会がある。比較的低コスト。	比較的新しい媒体であるため、国によっては利用者が少ない。
	ソーシャルネットワーキング・サービス	人と人とのつながりを促進・支援するコミュニティを活用できる。情報の地域間格差を解消できる。	加入しているサービスの利用者に対象が限られる。

出典：Philip Kotler & Gary Armstrong「Principle of marketing ver.9」をNTTデータ経営研究所にて加筆修正

図表 20　主な媒体タイプのプロフィール[18]

[18]出典：PEARSON　「コトラー＆ケラーのマーケティング・マネジメント第 12 版」p714-717

(2) 既存の事例調査

自己の実施状況を国民向けに広く客観的に認識できる媒体の配布方法について、既存の事例を調査した[19]。

その結果、自己診断チェックリストの媒体としてパンフレットを用いるもの、それらを PDF 化してウェブ上に掲載する配布方法を用いるもの、自己診断チェックリストをウェブシステムとして提供するものがあることが分かった。

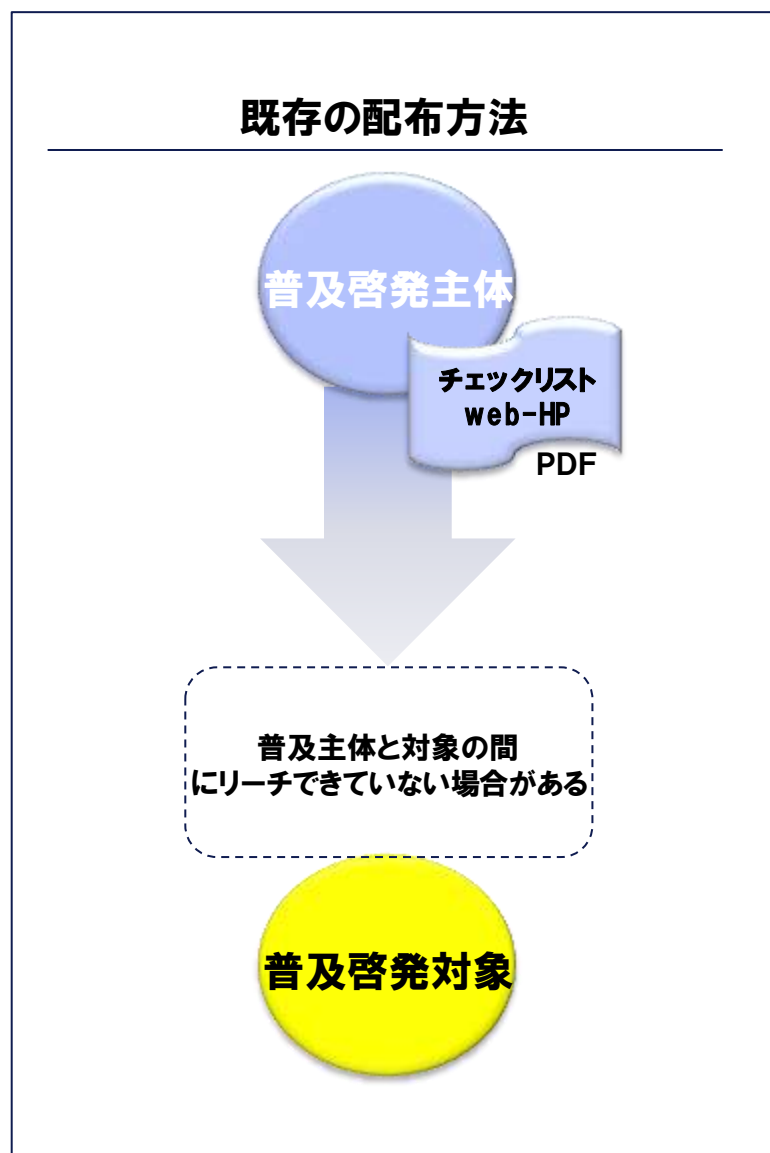
パンフレットの配布に加え、PDF 化しデジタルメディアを活用することは、より広範囲に低コストで配布を可能としている。PDF をウェブに掲載する手法を選択したことで、デジタル機器の利用に慣れていない人にも PDF を印刷し、紙媒体で自己診断チェックリストを届けることができるようにしている。本検討のように普及啓発対象者が広範な場合、本手法は上記の観点で有効であると考えられる。

配布方法	健康管理	人材育成	組織管理	情報セキュリティ
	Awareness	Response	Response	Response
事例	事例A,B,C	事例D,E	事例F	事例G
目的	•労働者に自分自身の健康状態を気付かせ、自己管理（改善）を行ってもらうため	•教育者が自己の指導スキルの現状を再認識し、スキル向上に努めさせるため	•経営者自ら経営状況を分析し、問題を見つけ自主的な改善努力を行うため	•企業を対象に外部からの不正アクセスを予防するとともに、問題が生じた際の被害を軽減するため
媒体配布方法	【アナログメディア】 •新聞掲載 •パンフレット作成 【デジタルメディア】 •PDF型パンフレット（web上に掲載） •チェックリストwebサイト	【アナログメディア】 •パンフレット作成 【デジタルメディア】 •PDF型パンフレット（ウェブ上に掲載）	【アナログメディア】 •パンフレット作成 【デジタルメディア】 •PDF型パンフレット（ウェブ上に掲載）	（アナログメディア） •パンフレット作成 （※15ページ程度で且つ具体的内容を記載） 【デジタルメディア】 •PDF型パンフレット(web上に掲載) •エクセル型パンフレット(web上に掲載)

図表 21　自己診断チェックリスト　配布方法事例（抜粋）

[19] 調査結果は、「別添資料 5　国内事例集」、「別添資料 6　海外事例集」に取りまとめている。

事例を図式化すると、図表 22 のように整理できる。

その結果、既存の配布方法は普及啓発主体の取組みが一方向的で、普及啓発対象者に届いているのか確認できない状況にあることが懸念される。一方、普及啓発対象者の視点からは、公開しているポイントを知らない場合、普及啓発主体の提供内容にリーチできないことが懸念される。

図表 22　既存の配布方法

(3) 有識者との配布方法に関する検討結果（配布方針）

自己診断チェックリストの配布方法は、普及啓発対象者にリーチしなければ意味がない。一方でリーチするためには、いくらでも予算をかけられるというものでもない。これまでの普及啓発主体の取組みを前提に、より普及啓発対象へのリーチを高める配布方法を、上記事例調査及び有識者との検討会を踏まえ、ポイントを以下のとおり整理した。

・情報セキュリティ分野の普及啓発の取組みを既に実施している組織がある
・普及啓発対象者にリーチしやすい機関・組織には、製品を販売する店（販売店）や、実際に製品の問合せ元となる製品ベンダーなどが存在している。
・情報セキュリティに関する取組みは、販売店だけでなく、情報セキュリティ資格試験団体や、パソコンスクール、地方自治体等の組織が行っている。

その結果、自己診断チェックリストの配布方針として、既存の普及啓発主体の取組みを活かし、いかに普及啓発対象者にリーチ先（普及啓発主体）を知らせるかに焦点を当てることとした。具体的には、情報セキュリティ分野の普及啓発の取組みを行っている組織・団体等の協力の下で、自己診断チェックリストの配布の仕組みを構築することである。

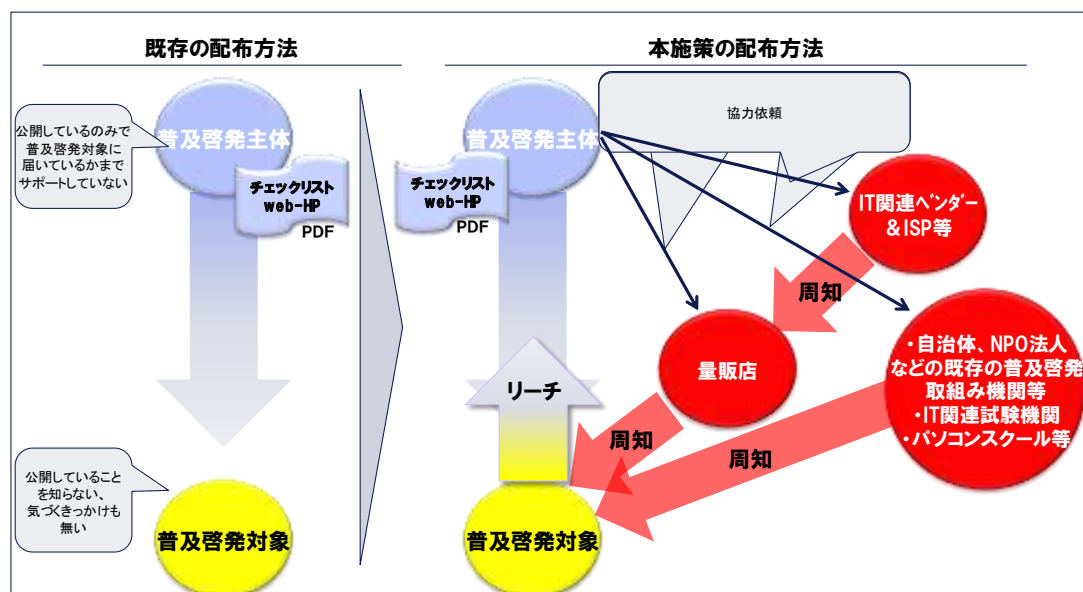
(4) 自己診断チェックリスト配布方法

本検討では、配布方針を受けて、既存の普及啓発主体の取組みを活かし、情報セキュリティ分野の普及啓発の取組みを行っている組織・団体等の協力の下で、自己診断チェックリストの配布の仕組みを構築することを提言する。

まず普及啓発主体は、ウェブに自己診断チェックリストを PDF 形式等で公開する。加えて、普及啓発主体は、情報通信機器や情報セキュリティ関連ベンダや販売店、情報セキュリティの取組みを行っている関係自治体担当部署や NPO 法人、情報セキュリティ関連の試験機関などから協力先を探し、当チェックリストの配布や掲載アドレス先の周知をしてもらえるよう協力を仰ぐ。

この体制によって、自己診断チェックリストの内容に国民が接しやすい環境づくりを推進する。

有識者の検討会においては以下のような具体例も示された。

情報通信機器や情報セキュリティ関連ベンダについては、自己診断チェックリストをベンダの扱う製品の取扱説明書内に取り込んでもらったり、パッケージに自己診断チェックリストの掲載先 URL を掲載してもらえるような取組みが考えられる。家電量販店については、製品を購入した人に、紙媒体で自己診断チェックリストや自己診断チェックリストの掲載先 URL を記載した印刷物を配布してもらえるような取組みが考えられる。情報セキュリティの取組みを行っている関係自治体や NPO 法人、パソコンスクールなどについては、既存の普及啓発活動の一環に自己診断チェックリストを取り入れてもらえるように、また IT 関連試験機関については、試験問題集に自己診断チェックリストを掲載してもらうことなどが考えられる。

図表 23　既存の世の中の事例配布方法と本施策の配布方法

2.4. 自己診断チェックリスト(案)

(1) 自己診断チェックリスト（赤版）

本検討の結果は、「別添資料１　自己診断チェックリスト(赤版)」にまとめた。

(2) 自己診断チェックリスト（黄版）

本検討の結果は、「別添資料２　自己診断チェックリスト(黄版)」にまとめた。

3.　高齢者向け資料の作成に関する検討

3. 1. 高齢化社会における情報通信機器を利活用する有益性

　我が国では、近年急速に高齢化が進行し、5 人に 1 人が高齢者という人口構造になるなか、高齢者の家族構成にも変化が生じており、約半分の高齢者が一人暮らしまたは夫婦のみで生活を送る地域社会もある。

　このような一人暮らしまたは夫婦暮らしの高齢者は、他の家族構成の世帯に較べて、孤独や健康、経済面に不安を抱えている。このため、友人知人との交流や健康、経済面に役立つ情報の提供・交換を効率的に行える情報通信機器が、高齢者の不安を軽減し、ニーズに応える手段として有効であり、その利活用への期待が高まっている[20]。

　インターネットを活用した暮らしは、自宅にいながらにしてパソコン等の情報通信機器を媒介として人とコミュニケーションしたり、欲しい情報を収集することを可能とする。情報通信機器は指先等で操作するだけで、インターネットにアクセスできる特性から、身体的ハンディや時間的・空間的ハンディを克服できる有益かつ便利な仕組みでもある。加えて、平時だけでなく災害時には、必要な情報を手に入れることにより、自身の命を守るツールと成り得ることが判明した。このことから、情報通信機器は平時には、孤独や健康、経済面に不安を抱える高齢者のニーズに応えたり、身体機能の低下や障害の有無に関係なく自立的な生活の維持を可能とする、重要な仕組み[21]である。また有事には、自身の命を守るツールであるといえる。

　このため、情報セキュリティを考えるとき、地域社会の高齢者の位置付けを無視することはできない。高齢者にとって、情報通信機器は有益であるから、今後も利用者が増加することが想像できる。そのことは同時に、高齢者向けの情報セキュリティリテラシー向上も併せて重要になることを意味する。

　そこで、本検討では、高齢者に対する情報セキュリティ普及啓発のための資料作成に向けた検討を行う。

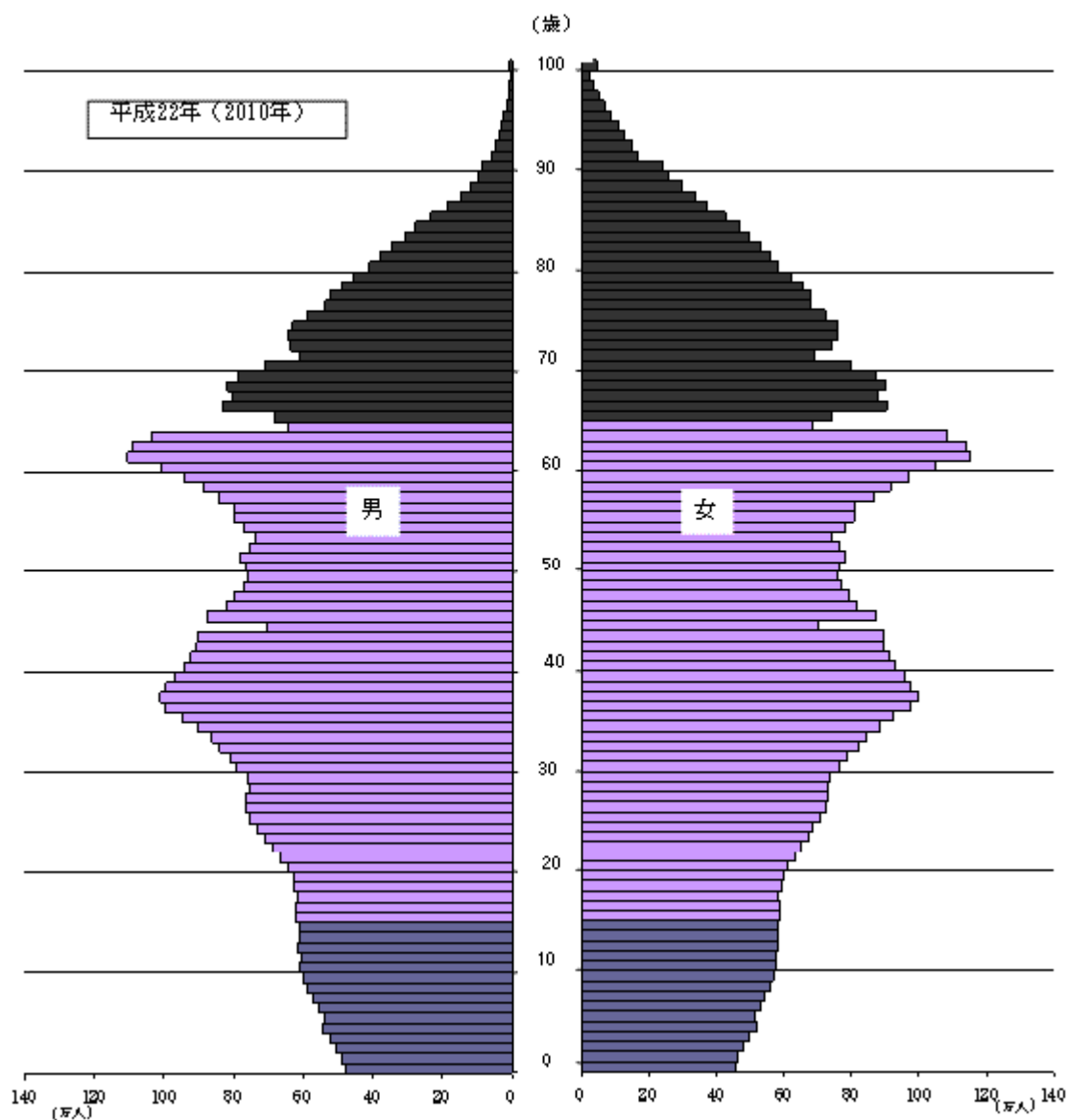
　本章では、高齢化社会における高齢者の生活実態とそこでの情報通信機器の利便性を明らかにする。

---

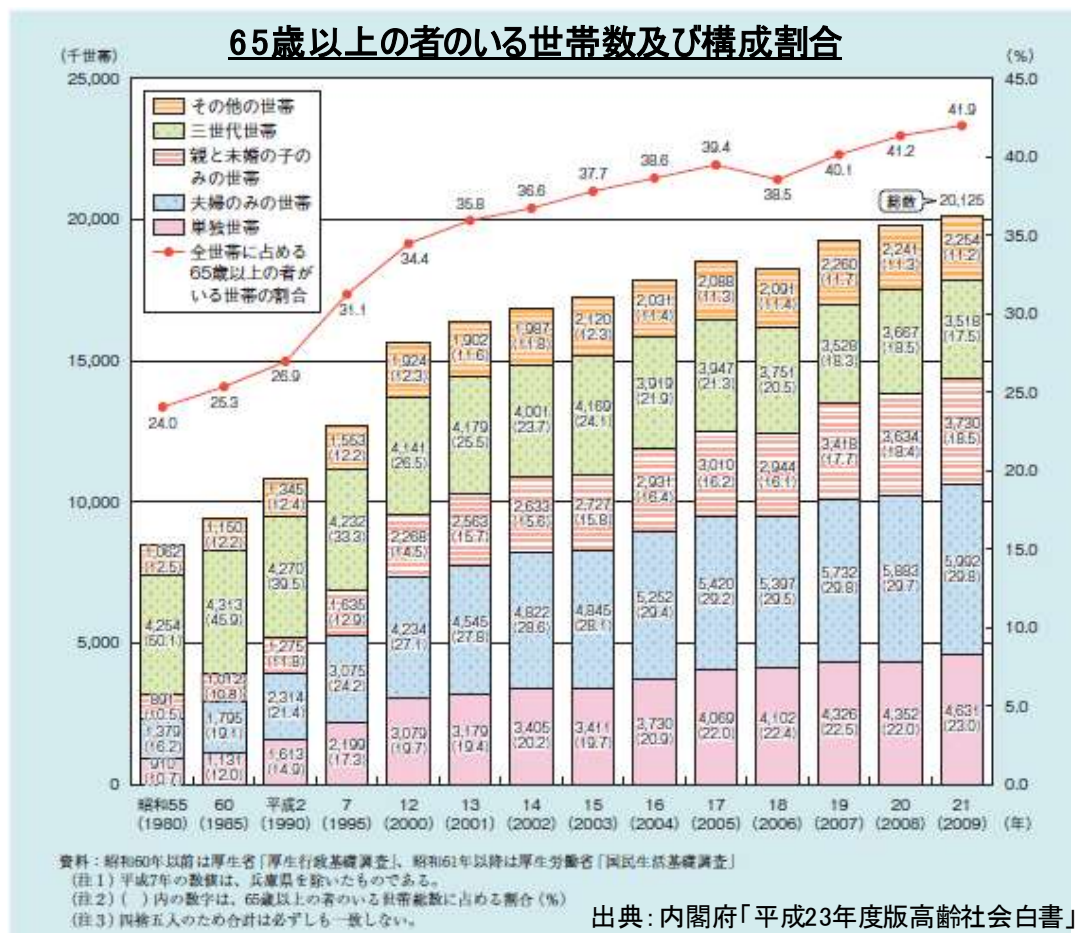
[20]総務省「平成 22 年度版　情報通信白書」第 1 章　ICT による地域の活性化と絆の再生　⑵高齢者のインターネット利用状況と利用促進の課題

[21] 上記脚注と同様

(1) 高齢者人口動向

日本の高齢者人口は、総務省の平成 23 年度統計において 2,980 万人と報告されている。総人口に占める割合は 23.3%で過去最高であり、5 人に 1 人が高齢者という人口構造である[22]。(図表 24 は、総務省統計局が公開している最新の人口ピラミッド図)

図表 24　平成 22 年　人口ピラミッド図[23]

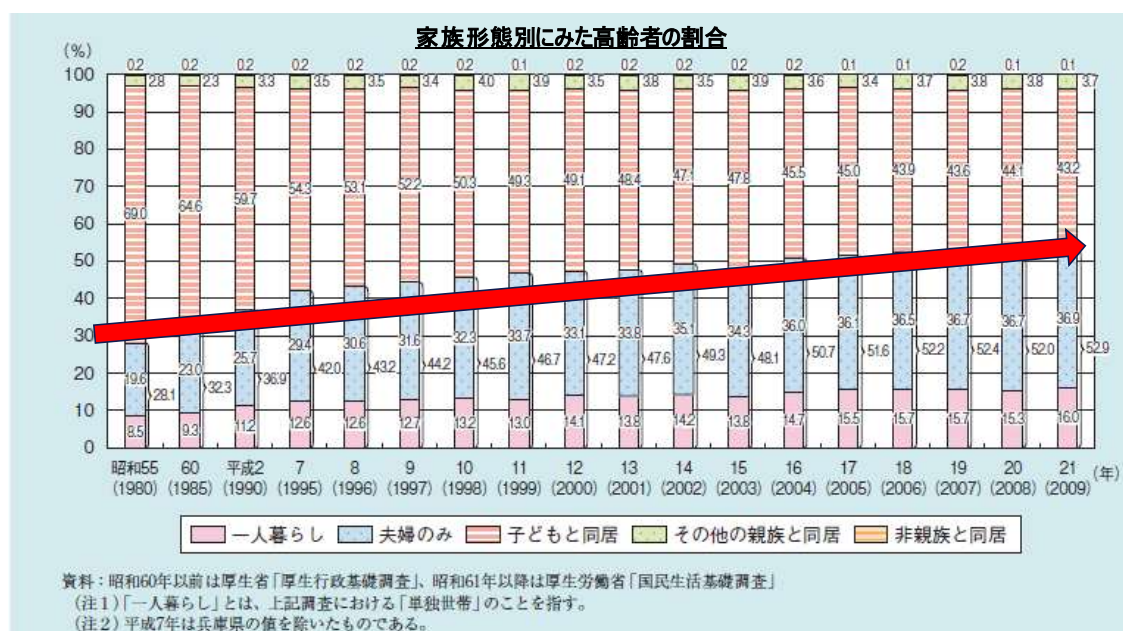
[22]出典：総務省統計局　「平成 23 年度人口統計」
[23]出典：総務省統計局　「平成 22 年人口ピラミッド」
http://www.stat.go.jp/data/kokusei/2010/kouhou/useful/u01_z19.htm

図表 25 にみるように、65 歳以上の高齢者がいる世帯の割合も年々増加している。

図表 25　65 歳以上の者のいる世帯数および構成割合[24]

---

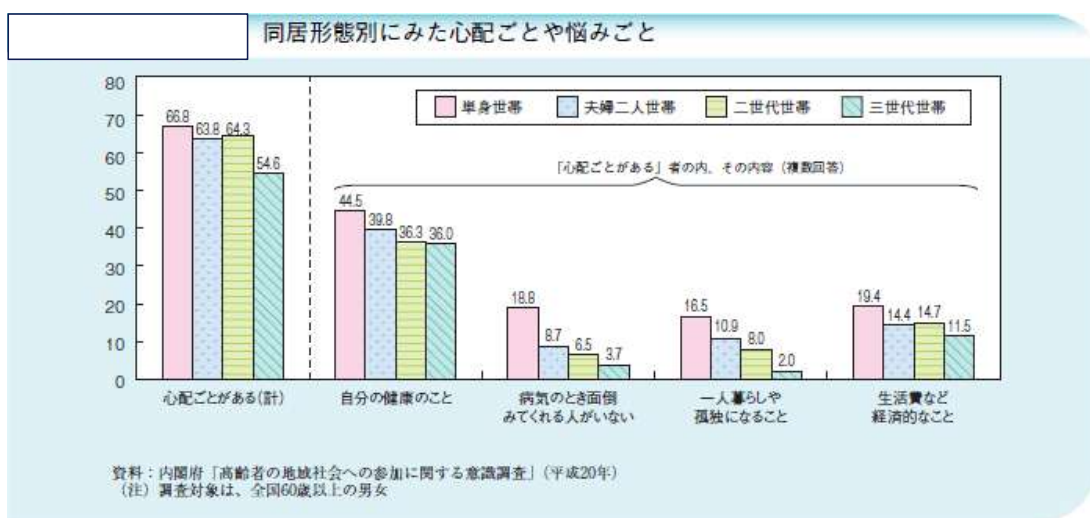
[24]出典：内閣府　「平成 23 年度版高齢社会白書」

(2) 高齢者の家族形態

高齢化が進行するなか、高齢者の家族形態にも変化があり、子供との同居が減少する一方で、一人暮らしまたは夫婦のみの世帯が増加している。図表26 をみると、子供との同居は、1980 年時点では 69%と半数以上であったが、2009 年時点では 43.2%と半数を割り、大幅に減少している。一方で、一人暮らしまたは夫婦のみの世帯は 1980 年時点で 28.1%だったが、2009 年には約 2 倍の 52.0%まで急増していることが分かる。

図表 26　家族形態別にみた高齢者の割合[25]

[25]出典：内閣府　「平成 23 年度版高齢社会白書」

(3) 高齢者の心理的側面

家族形態別に高齢者の心配ごと、悩みごとをみる（図表 27）と、一人暮らしの高齢者は、他の世帯と比べて孤独、健康、経済面などの心配ごとを持っていることが分かる。独立行政法人国民生活センターの話では、「高齢者は孤独、健康、お金の 3 つの大きな不安を持っている」と指摘している。このような心理状況にある高齢者は、友人や知人との交流や健康、経済面に役立つ情報を求めていると考えられる。

図表 27　同居形態別にみた心配ごとや悩みごと[26]

[26]出典：内閣府　「平成 23 年度版高齢社会白書」

(4) 高齢者の心の支え

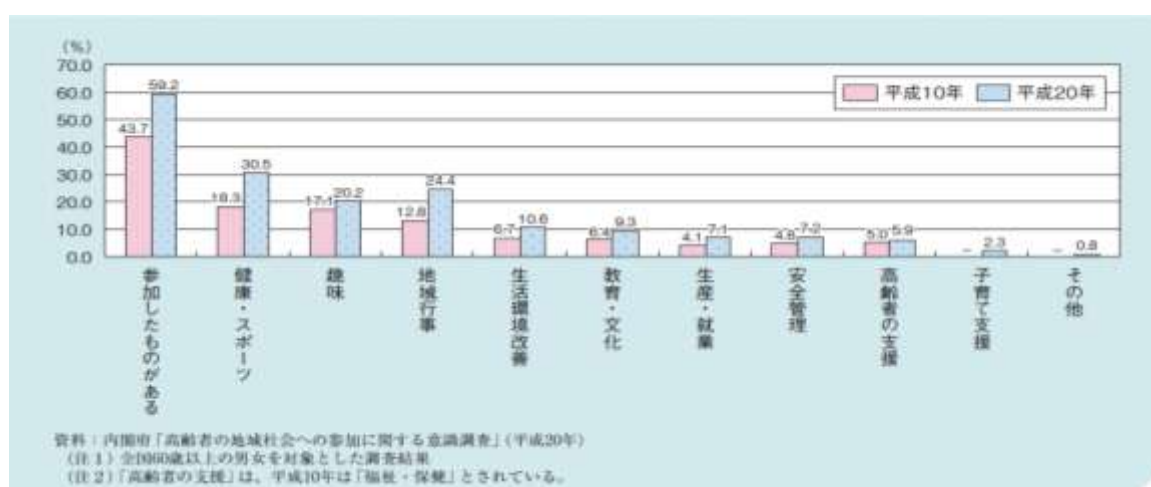
高齢者の心の支えとなっている人について図表 28 をみると、孤独や健康、経済面などの様々な悩みを抱えているなかで、高齢者は配偶者やパートナー、子供を心の支えとしている、という回答が多い。一方で、友人や知人を頼りにしている人は 13. 1%となっており、友人知人との交流は配偶者やパートナーに較べて少ないようである。

図表 28　高齢者の心の支えとなっている人[27]

[27]出典：内閣府　平成 23 年度版高齢社会白書

(5) アクティブシニア層とノンアクティブシニア層

高齢者の行動面に着目すると、元気なお年寄りと、身体機能の低下に伴い外出が億劫になってしまった人等に分かれる。前者をアクティブシニア層、後者をノンアクティブシニア層と定義する。

進展する高齢化では、各層ともに人数が増えている。すなわち、高齢者のなかでもアクティブな活動を好む人が増えており、図表 29 からは、どの活動項目においても平成 10 年度から平成 20 年度にかけて増加傾向にあることが確認できる。その他にも、ボランティア活動にも非常に意欲を示しており、高齢者自身が老後に活躍する場を求める傾向があることが把握できる。

図表 29　　高齢者のグループ活動への参加状況[28]

[28]出典：内閣府　「平成 23 年度版高齢社会白書」　第 2 節 5 項　高齢者の社会参加状況

(6) 情報通信機器の利活用が高齢者にもたらす利便性

高齢化が進む社会において、高齢者の不安や身体的ハンディを克服する手段として、情報通信機器の利活用がもたらす利便性に期待が高まっている。

情報通信機器は、そもそも時間的・空間的ハンディを克服することが可能である点と、その特徴から身体的ハンディの克服を支える点、さらに先の東日本大震災等の教訓から指摘された、有事の際に自身の命を守る点から高齢者に有益なツールであることが整理できる。

情報通信機器を活用した暮らしは、自宅にいながらにしてインターネットを媒介に、人とコミュニケーションをしたり、欲しい情報を収集することを可能にする。

また、人間は加齢に伴い筋力が衰え身体的な機能が低下する。病気にかかりやすくなったり、病気が治りにくくなるなど、健康面にも不自由が生じる。情報通信機器は指先等で操作するだけで、インターネットの接続先にアクセスして様々なサービス等を受けられる機能を有しているため、加齢に伴う機能低下を補完したり、コミュニケーション手段を確保したり、様々な側面で支えるものである。今後、情報通信機器の普及が進んだ際には、結果として、身体機能低下や障がいの有無に関係なく、自立的な生活を維持できることにより、社会厚生の増大を実現することになると考えられる[29]。

情報通信機器の利活用は、平時に有益なだけではない。先の震災では、停電や携帯回線の輻輳などにより、テレビや携帯電話からの情報収集が困難を極めた。このような状況の中で高齢者は、避難所がどこにあるか分からなかったり、いつどこに避難物資が配送されるか分からなかったりなど、情報弱者となるケースが目立った。

一方で、スマートフォンなどの携帯通信端末を所有していた人は、固定電話と比べて早期に通信可能となり、インターネットなどを利用して情報を収集できる環境となった。このことは、震災に関する情報収集や、行方不明になった親族の安否確認などのコミュニケーションツールとしてスマートフォン等を利用することが有益であったことを示している。

このような情報通信機器は、高齢者にとっても有事の際に命を支える情報を得るための有益なツールとなる。

[29]出典：総務省　平成 22 年度版　情報通信白書　第 1 章　ICT による地域の活性化と絆の再生　(2)高齢者のインターネット利用状況と利用促進の課題

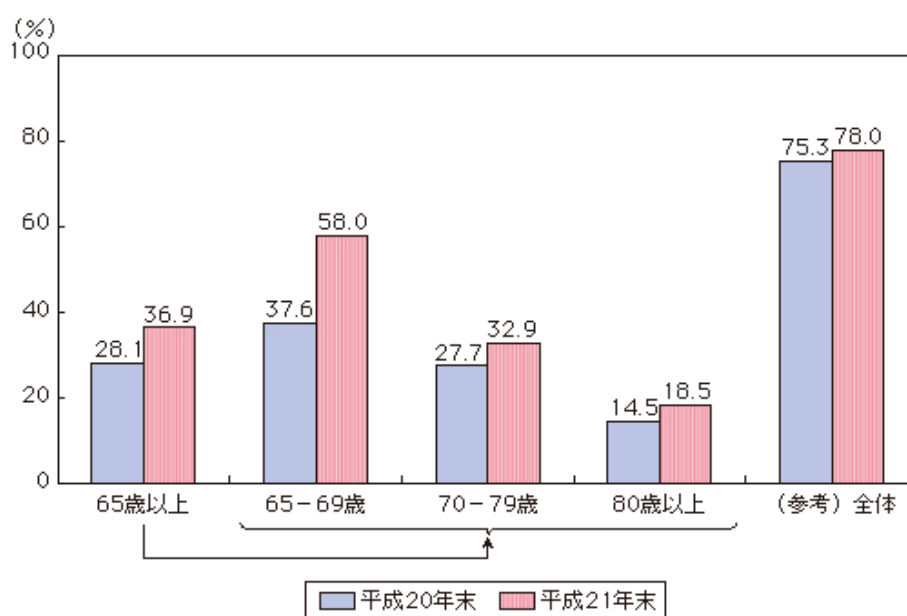
3.2. 普及啓発対象者像

高齢者にとって、情報通信機器は有益であるから、今後も高齢者のインターネット利用率は増加傾向に進むことが想像できる[30]。そのことは同時に、高齢者向けの情報セキュリティリテラシー向上も併せて重要になることを意味し、実際にインターネットを利用している高齢者は、利用に際して「ウイルスの感染」、「プライバシーの保護」、「情報流出の危険性」などを不安に感じている。

本検討では、このような高齢者のインターネット利用実態について整理したうえで、情報セキュリティの普及啓発対象者像を明確にする。

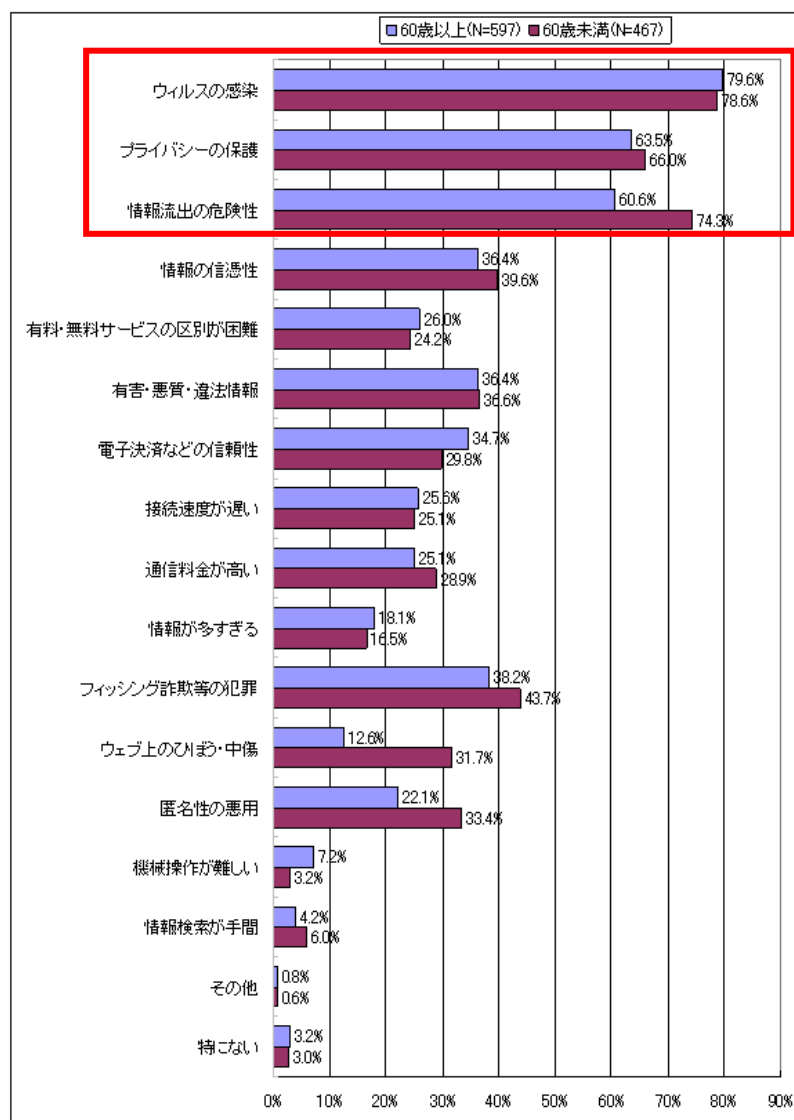
[30]高齢者のインターネットの利用率はわずか30%程度であり、残りの約70%はインターネットをまだ利用していないのが現状である。

(1) 高齢者のインターネット利用状況

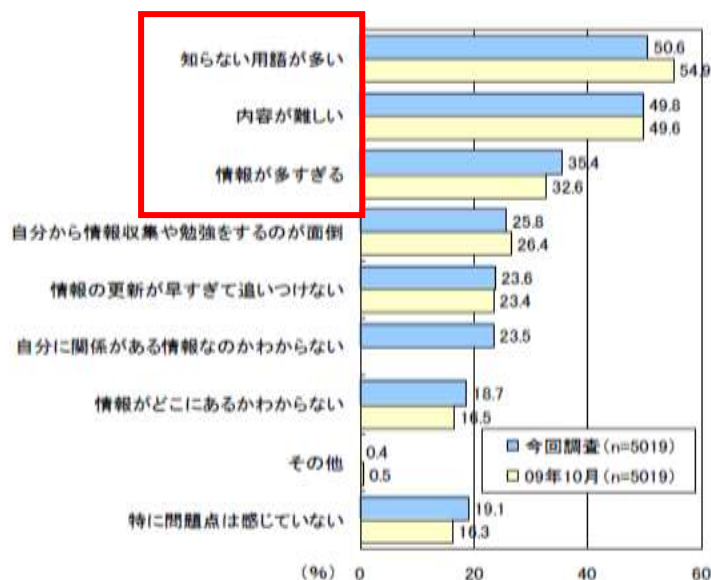
高齢者のインターネット利用状況について図表 30 をみると、高齢者のインターネット利用率は増加傾向にあるものの、平成 21 年末時点では平均 36.9%であり、全体平均の 78.0%に対しては、その半分にも満たない。73.1%もの高齢者は、インターネットを利用していないことになる。本検討では、インターネットを利用している高齢者層を“デジタルアクティブ層”、インターネットを利用していない高齢者層を“ノンデジタル層”とする。

図表 30　高齢者のインターネット利用率[31]

[31]出典：総務省　平成 21 年通信利用動向調査

(2) 高齢者がインターネット利用時に感じる不安

デジタルアクティブ層がインターネット利用時に感じる不安として、「ウイルスの感染」、「プライバシーの保護（プライバシー情報の漏えい）」、「情報流出の危険性」が上位 3 位までに挙げられる（図表 31）。

図表 31　高齢者がインターネット利用時に感じる不安[32]

[32]出典：総務省　平成 21 年通信利用動向調査

こうした状況の背景として、図表 32 では、情報セキュリティ情報を収集する際に「知らない用語が多い」、「内容が難しい」、「情報が多すぎる」などを問題点として感じていることが挙げられる。

図表 32　情報セキュリティに対する取組み意識[33]

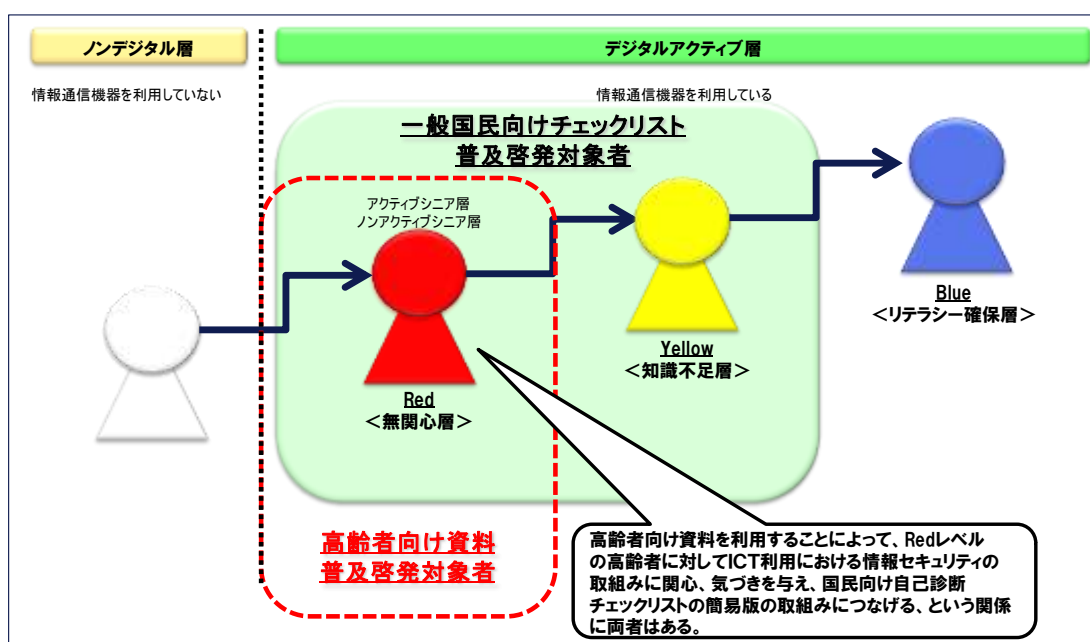
このことから高齢者は、インターネット利用時には自身の不安に対する対策を講じたいにもかかららず、内容が高度で難解なこともあり十分な対策に取り組めていないことが伝わってくる。

[33]出典：独立行政法人情報処理推進機構 IPA「情報セキュリティの脅威に対する意識調査　報告書」平成 2010 年 12 月

(3) 普及啓発対象者像

高齢者のインターネット利用実態（図表 31）を踏まえると、デジタルアクティブ層の 70%程度の人が、情報セキュリティ脅威に対して不安にあることが分かった。また、取り組みたくても、用語が難解で、情報量が多すぎることも分かった。このことは、情報セキュリティ脅威に対する対策の入り口でつまずいている状況にあると推察できる。

そこで、本検討の普及啓発対象とする高齢者層は、情報セキュリティの取組みの入り口でつまずいている“Red”を構成する高齢者とし、一般国民向け施策と併せて、きめの細かい情報セキュリティの普及啓発資料を提供することとする。すなわち、高齢者向け資料の普及啓発対象者像は、情報通信機器を利用しているデジタルアクティブ層のうち、情報通信機器に関する知識が乏しく、情報通信機器の利用時に何が安全で何が危険か、何をすればいいのか理解できていない高齢者(“Red”層)とする。

なお、デジタルアクティブ層で“Red”の高齢者は、活動的なアクティブシニア層と在宅志向型のノンアクティブシニア層で構成されるため、高齢者向け資料の配布の際には、両者にリーチできるよう留意する必要がある。

図表 33　高齢者向け資料　普及啓発対象

3.3. 高齢者向け資料の作成指針

高齢者向け資料に盛り込む事項は、本検討の普及啓発対象者（”Red”を構成するアクティブシニア層、ノンアクティブシニア層）にリーチする媒体、関心を引きつける記載内容であることを主眼において作成方針をまとめる。

本検討では、活動範囲が異なる普及啓発対象者にリーチできるよう、活動的なアクティブシニア層が外出時に気付きを得られる資料（以下、外出時リーチ資料）と、アクティブシニア層もノンアクティブシニア層も共に読み物として利用できる資料（以下、在宅時等リーチ資料）の 2 種類を用意する。それぞれの資料の作成方針は、普及啓発目的、形式、内容、の 3 構成で整理する。

本節では、はじめに普及啓発対象者に提供する高齢者向け各資料の目的について整理したうえで、形式、内容について既存の取組み事例調査等を行い、そこから得られた知見等をまとめる。その結果を受けて、各高齢者向け資料作成指針を示す。

(1) 提供する資料の目的と両資料の関係

①提供する資料の目的

普及啓発対象者（”Red”を構成するアクティブシニア層、ノンアクティブシニア層）は、一般国民向けの取組みで整理したようにアウェアネスが普及啓発の目的であることは変わらない。ここで整理すべきは、普及啓発対象者に提供する資料の目的である。

本検討の対象者は、活動範囲が異なる層に分類していることから、外出時にリーチできる資料内容と、在宅時のような比較的時間をとれる環境にリーチする資料内容とでは、資料に盛り込むメッセージが異なる。そこで、アクティブシニア層を主要な普及対象とする前者の外出時リーチ資料と、ノンアクティブシニア層も利用視野に入れた後者の在宅時等リーチ資料の目的を以下に整理する。

アクティブシニア層は、活動的であることから、自宅だけでなく、外出時に情報に触れる機会がある。そこで、外出時にリーチする資料（外出時リーチ資料）は、外出時に目に触れ、情報セキュリティに関心を引き起こすきっかけとなることを目的とする。

アクティブシニア層およびノンアクティブシニア層の両者にリーチする資料（在宅時等リーチ資料）は、自宅等で時間をかけて内容を読めることを前提として、インターネット利用時に何が安全で何が危険か、何を行うべきなのか、に関して高齢者の生活面から気付きを与えることを目的とする。ここで関心が喚起された後は、自己診断チェックリスト（赤版）の利用へ進むことを利用の目的とする。

②両資料の関係

外出時リーチ資料と、在宅時等リーチ資料の関係を以下に整理する。

外出時リーチ資料は、アクティブシニア層の目にとめて、情報セキュリティに関心を持ってもらう資料である。

外出時リーチ資料により喚起した関心に基づいて、具体的な内容（利用シーンに基づいてやるべき事）を知ってもらうために利用できる資料が、在宅時等リーチ資料である。

外出時リーチ資料は、情報セキュリティリテラシー向上のための「きっかけづくり」であり、在宅時等リーチ資料は、自身がやるべき事を理解する「確認資料」のような関係にある。

(2) 高齢者向け資料に盛り込むべき内容および形式

高齢者向け資料に盛り込むべき事項は、資料の目的に照らし合わせて、内容、形式について既存の取組み事例調査等を行い、そこから得られた知見等をまとめる。

内容とは、普及啓発内容として記載事項（理解しやすい用語の使い方含む）であり、形式とは、記載事項をどのような様式（レイアウト含む）で、どの程度の記載ボリューム（分量）かを対象とする。

①既存の取組み事例

高齢者層にリテラシー向上を行う国内外の事例を調査した[34]。

その結果、高齢者向け資料に盛り込む内容について既存の事例は、図表 32 にあるように、情報量が多く、かつ用語が難解であることが分かった。

形式については、ベストプラクティスといえるような業界横断的な作成マニュアルのようなものの存在は確認できなかった。そこで、各普及啓発主体へインタビュー[35]したところ、各普及啓発主体の目的に応じて、試行錯誤しながら形式を取りまとめていることが分かった。

一方、媒体については、アナログメディアとデジタルメディアだけでなく、イベント型の普及啓発活動を組み合わせて、多角的に高齢者へと普及啓発活動を実施している事例が散見された。

以下の図表 34 に、事例調査結果をコンテンツ作成、および配布媒体の観点から整理した。

[34] 調査結果は、「別添資料 5　国内事例集」、「別添資料 6　海外事例集」に取りまとめている。
[35] 東京都内の区役所、団体、当へ電話または訪問によりインタビューを行った。

	地上放送のデジタル化	振り込め詐欺	介護	財政管理
	事例(A)	事例(B)(C)	事例(D)	事例(E)
目的	•国民をアナログ放送から地上デジタル放送へと移行させるための告知、支援するため	•高齢者の大切な財産を振り込め詐欺の被害から守るため	•高齢者と障害者、その介護家族の生活の質の向上を支援するため	•高齢者を対象に、財政管理のヒントを提供し、彼らの生活の安全を保ち、自立の手助けをするため
コンテンツ作成の観点	•地上デジタル放送のメリット(画質向上など)を資料に反映 •地上デジタルへの移行を急かすために、移行期間を明確に表示 •地上デジタルへの移行方法が分からない人へ、相談先を伝達	•振り込め詐欺を自分事として捉えさせるために、手口や実例をウェブサイト上で公開 •詐欺以外の事例として、不法侵入や窃盗、悪質商法、交通事故などの被害も合わせて啓発 •振り込め詐欺の被害を例示するだけでなく、対策まで踏み込んで説明	•高齢者が自立した生活を送れるようなノウハウ情報を提示 •日常生活の飲食、移動操作、失禁、床ずれ、発作等の情報を共有する	•予算の立て方、詐欺の避け方、福祉手当の申請方法など財政管理のヒントを資料に反映 •高齢者がオンランセミナーを快適に利用できるように、ツールキットの使い方を詳しく説明 •財政判断自己診断チェックリストを高齢者向け資料に掲示
配布媒体	(アナログメディア) •TV•CM•ニュース •雑誌 •ポスター •パンフレット •広告•チラシ etc (デジタルメディア) •ウェブサイト •インターネット広告 etc (イベント型) •屋外イベント •キャンペーン活動 etc	(アナログメディア) •TV•CM•ニュース •雑誌 •ポスター•パンフレット (金融機関•自治体の協力) •広告•チラシ etc (デジタルメディア) •ウェブサイト •インターネット広告 etc (イベント型) •屋外イベント •キャンペーン活動 etc	(アナログメディア) プレゼンテーションppt資料 (デジタルメディア) •ウェブサイト •動画サイト (イベント型) •ビデオ電話との対話 •コールセンター職員による教育支援	(アナログメディア) •プレゼンテーションPDF資料 •ハンドブック •トレーニングガイド (デジタルメディア) •ウェブサイト (イベント型) •オンラインセミナー
示唆	●**コンテンツ作成の観点** いずれの事例も、業界横断的なマニュアルのようなものは存在せず、各組織毎に目的に応じて適切なコンテンツ作成の観点を設定している ●**様式作成の観点** 事例ごとに規定されていなかったが、アナログメディアとデジタルメディアだけでなく、イベント型の普及啓発活動を組み合わせて、多角的に高齢者へと普及啓発活動を実施している事例が散見された			

図表 34　事例調査結果整理

上記事例のうち、地上放送のデジタル化、振り込め詐欺については、テレビの CM やニュースなど広域へと情報発信できる媒体を採用していた。両事例の予算を調査したところ、地上放送へのデジタル化は平成 22 年度予算で 8.4 億円程度、振り込め詐欺は犯罪対策関連経費における平成 22 年度予算で 200 万円程度である。

この他、アクティブシニア層が訪問するフィールド[36]を調査した結果、高齢者にリーチするための媒体として、冊子やリーフレット、ポスターなどの掲示物が設置されていることが分かった。また、在宅中の高齢者にリーチする媒体には、新聞、雑誌、リーフレットなど、ポスターに比して情報量の豊富な媒体が配布されている様子が確認できた。

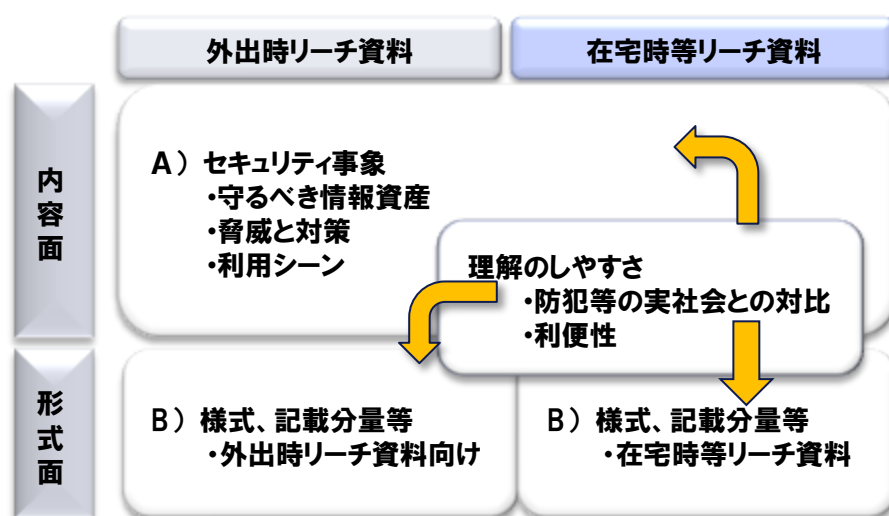
		フィールド調査結果	
		利用媒体	インタビュー結果
在宅時	インターネット非利用	・テレビCM ・新聞広告 ・ダイレクトメール ・雑誌広告 ・回覧板 ・リーフレット ・冊子	―――
在宅時	インターネット利用	・インターネット広告 ・テレビCM ・新聞広告 ・ダイレクトメール ・雑誌広告 ・回覧板 ・リーフレット ・冊子	―――
外出時	学校 公民館	・イベント ・講座開設	某商工会議所に電話にてインタビューを実施したところ、高齢者向け資料のノウハウとして整理した物はなく、その都度配布物作成を関係者と検討して作成している　(2011/12/21)
外出時	病院 介護施設	・配布物整備 ✓冊子 ✓リーフレット ✓掲示物(ポスター)	某総合病院にてインタビューを実施したところ、特にノウハウとして整理した物はなく、その都度配布物作成を関係者と検討して作成しているとの回答を受けた（2011/12/21）
外出時	役所	・配布物整備 ✓冊子 ✓リーフレット ✓掲示物(ポスター) ・講習会開設 ・支援体制整備 ✓相談員 ✓支援員	都内某区役所に訪問してインタビューを実施したところ、特に意識しているというものは無いものの、掲示物である以上、読みやすく、理解しやすい内容を意識している程度、との回答を受けた(2011/12/28)
外出時	銀行 郵便局	・配布物整備 ✓冊子 ✓リーフレット ✓掲示物(ポスター)	―――
外出時	商店	・配布物整備 ✓冊子 ✓リーフレット ✓掲示物(ポスター)	―――
外出時	その他	・屋外広告 ・ラッピングバス ・自治体掲示版 ・カレンダー	某情報セキュリティ協会に訪問してインタビューを実施したところ、高齢者を意識して資料を作るということは無いが、一般国民誰でも読みやすいように文字を大きくする、専門用語は使わない等の工夫はしているとの回答を受けた。(2012/1/9)

図表 35　フィールド調査結果

[36] 公民館、病院、役所、等

②有識者との内容および形式に関する検討結果

上記、既存の取組み事例の結果、高齢者向け資料に盛り込むべき内容および形式を参考にしつつも、高齢者の理解のしやすい資料づくりとは何かを高齢者の価値観や各種ハンディを考慮したうえで、有識者との検討を経て具体化した。

資料に盛り込むべき内容は、自己診断チェックリストの検討の際に整理した観点（　A）セキュリティ事象　）に対して、高齢者が理解しやすいか、興味を喚起する内容か、に着目して見直した。形式（　B）様式、記載分量等　）についても、高齢者が理解しやすいか、に着目して見直した。

図表 36　高齢者向け資料に盛り込む観点

A)　情報セキュリティ事象の見直し

高齢者に普及啓発する情報セキュリティは、自己診断チェックリストに盛り込む内容を踏襲するものの、高齢者の関心を得るためには、まず情報セキュリティが自身に関わることである、と認識してもらう必要がある。

高齢者は老後の不安(「お金」、「健康」、「孤独」、以下 3 大不安)を抱えている特徴があることから、自身の不安と守るべき情報資産の関係を改めて確認した。また、高齢者向けに見直すべき事項がないか、有識者との検討結果を整理した。

A)-1　高齢者が守るべき情報資産

高齢者が守るべき情報資産は、自己診断チェックリストの章で整理した「守るべき情報資産」と異なるのか、若しくは同じなのかを整理する。また、高齢者が抱える 3 大不安と情報資産の各内容を関連付けることにより、高齢者が守るべき情報資産を明らかにし、情報資産が被害を受けた場合、自身にどのような苦痛が発生するのかについても整理した。

整理の結果、図表 37 が示すように、高齢者も一般国民同様に、どの情報資産についても情報セキュリティ被害にあうことで失った場合、自身の不安要素に直結するとともに、精神的苦痛や経済的苦痛を伴うことが分かった。このため、高齢者向け資料作成の際には、どの情報資産についても被害を受けないよう、普及啓発により、守るべき資産の重要性を伝える必要があることを確認した。

			3大不安			自身が受ける被害との関係	
			お金	健康	孤独	精神的苦痛	経済的苦痛
情報資産種別	個人情報	個人基礎情報		○		○	
情報資産種別	個人情報	個人属性情報		○		○	
情報資産種別	金融・財産情報		○	○		○	○
情報資産種別	思い出情報				○	○	

図表 37　情報資産を失うことによる影響と 3 大不安の関係

（参考）各不安要素と情報資産及び自身が受ける被害との関係

・お金：口座番号や金融機関のパスワード情報（金融・財産情報に該当）の漏えいは、自身のお金を失う危険に繋がるため、不安要素のうち、「お金」に直結する関係にある。金銭を失う被害が発生した場合には、精神的、経済的苦痛を伴う。

・健康：自身のプライバシー情報（個人情報に該当[37]）や口座情報（金融・財産情報に該当）の漏えいは、自身の精神状態に悩みを与えることに繋がるため、不安要素のうち、「健康」に直結する関係にある。プライバシー情報の被害が発生した場合は、精神的な苦痛を伴う。

・孤独：蓄積してきた写真や日記等の記録（思い出情報に該当）の喪失は、人生の記録を失うことになることから、不安要素のうち、「孤独」に直結する関係にある。過去の思い出を失うことは、精神的苦痛を伴う。

---

[37] プライバシー情報は、次の3つの条件全てを満たす情報。
⑴個人の私生活上の事実に関する情報
⑵一般の人に知られていない情報
⑶一般人の感受性を基準にして、通常は公開を望まない情報

これに対して、個人情報は、私生活上の情報であるかどうかや、公開を望むかどうかは関係なく、電話帳に掲載されている情報なども個人情報に該当する。
このため、プライバシー情報と個人情報は異なる概念であるが、プライバシー情報と個人情報は重なり合っている部分もある。

A)-2　脅威と対策

　高齢者に特化した脅威は情報セキュリティ上存在するのかについて整理した。

　その結果、図表 38 にあるとおり、情報セキュリティに関する被害は、どの年代においても差はなく、高齢者だけが受ける被害があるわけではないことが確認できた。むしろ、どの世代も「被害にあったことがない」、または「被害にあったかどうかわからない」と回答した人が多く、大多数は被害を認知できていない状況にあることが改めて把握された。

　したがって、脅威と対策については、自己診断チェックリストと同様の考え方を用いる。

図表 38　年代別・習熟度別　過去 1 年間の
情報セキュリティに関する被害・トラブル[38]

[38]出典：独立行政法人情報処理推進機構 IPA「情報セキュリティの脅威に対する意識調査　報告書」平成 2010 年 12 月

A)-3　利用シーン

利用シーンについても自己診断チェックリストと同様の考え方を用いる。

A)-4　その他考慮事項

有識者との検討の結果、以下の指摘があった。

・ 何ごとも、メッセージを出す際には、脅威というデメリットを全面に押し出されると、利用回避に向かう可能性があるため、情報セキュリティの普及啓発には、恐怖心を煽って利便性を損なうことないよう配慮が必要である

・ 情報セキュリティという実態の見えにくい世界はイメージしにくいため、情報セキュリティの普及啓発には、実社会の防犯の取組みなどと対比させることが関心を持ってもらうのに効果的である

A)-5　普及啓発の対象とする情報セキュリティ事象（まとめ）

上記 A)-1 から A)-4 までを踏まえて図表 39 に高齢者版情報セキュリティ事象一覧を整理する。

利用シーン		情報セキュリティ事象	外出時リーチ資料での取扱	在宅時等リーチ資料での取扱
1. 利用環境設定時		脅威：利用環境のセキュリティが設置されていない場合、各種攻撃、不正アクセス、不正利用の危険 対策：インターネット利用時のセキュリティツールの設置(ウイルス対策ソフトの導入、セキュリティパッチの適用、等)	➢1 ➢2	➢1 ➢2
2. 起動・立ち上げ時		脅威：機器の起動時は自分以外の第三者に機器を自由に利用される危険 対策：機器起動時のログインID・パスワード設定、等	➢2	➢2
3. サービス利用時		―――		
	① 企業・政府などのホームページ(ウェブ)・ブログの閲覧	脅威：OSやソフトウェアの脆弱性が修正されていない場合、不正アクセスやコンピュータウイルスなどの攻撃等 対策：セキュリティパッチの適用、ウイルス対策ソフトの更新、等	➢3	➢3
	② 企業・個人などのホームページ(ウェブ)・ブログでの個人情報のやり取り(④を除く)	脅威：個人情報の侵害・漏えい、紛失 対策：個人が特定される情報を安易に公開しない(公開範囲の制限)、個人情報が保存されたファイルには、暗号化やパスワードを設定、バックアップ、等	➢4	➢4
	③ 商品・サービスの購入・取引(⑤を除く)	脅威：なりすまし、詐欺による金融・財産情報の漏えい、紛失、等 対策：利用するネットショッピング先は信頼する友人の情報に基づいた利用、ネットバンキング用のID・パスワードは類推されにくいものの設定、管理、ネットバンキング利用履歴の消去、金融機関を名乗りネットバンキング用のID・パスワードの入力を促すメールが届いても安易に教えない、等	➢4 ➢5	➢4 ➢5
	④ 思い出情報(日記や各種記録)の作成公開時	脅威：プライバシーの侵害、等 対策：情報漏えいの可能性が伴うファイル共有ソフトを利用しない、インターネットに公開する写真や動画は、関係者に公開することの許可、公開時の情報取捨選択、バックアップ、等	➢4	➢4
	⑤ デジタルコンテンツ(音楽・音声、映像、ゲームソフトなど)の入手・聴取	脅威：ウイルス感染、等 対策：ウイルス対策ソフトの導入・パターンファイルの最新化、「ホームページの信頼性評価」を用いたサイトの利用	➢6	➢6
	⑥ ネットワークを介したゲームや家電機能の利用	脅威：①から⑤と同様の脅威が想定 対策：①から⑤と同様の対策を想定	–	
	⑦ 自身のブログなどの作成	脅威：②から④と同様の脅威が想定 対策：②から④と同様の対策を想定	②から④のなかで扱う	
	⑧ 電子メールの利用	脅威：電子メール受信時にはウイルス感染・成りすまし等の危険、送信時には誤送信・情報漏洩の危険 対策：身に覚えのないアドレスから届いたメールの添付ファイルは安易に開封しない、覚えのないアドレスから届いたメールには返信しない、電子メールを一括送信するときは、Bccで送付する	➢7	➢7
4. 自宅外への持出時		脅威：紛失・盗難 対策：貴重品を扱うように常に所在を意識した行動 USBの中のファイルにパスワードの設定、事前にデータバックアップ	➢8	➢8
5. 利用していない時(トラブル対応)		脅威：トラブル発生時には、どのように対応、どこへ連絡・相談してよいか分からない 対策：インターネットに有線で接続している場合、回線を抜く 一人で悩まず、誰かに相談する	➢9	➢9

図表 39　高齢者版情報セキュリティ事象一覧

B)様式、記載分量等

外出時リーチ資料の形式は、事例調査結果を踏まえ、有識者との検討会を経て以下に整理した。

・外出時に目に触れやすい媒体としてポスターが有効である
・ただし、ポスターはメッセージが１つしか掲載できないことから、数枚作成するか、カレンダー形式も考えられる
・メッセージは、川柳などの形式で作成すると読みやすい

在宅時等リーチ資料の形式は、同様に事例調査結果を踏まえ、有識者との検討会を経て以下に整理した。

・ポスターでは足りない具体的な内容を周知させるために、在宅時等の利用媒体としては、見開きページ程度のパンフレットが有効である
・記載内容は、恐怖心を煽って、情報通信機器の利用促進を阻害しないよう配慮すること
・視認性を意識して、字のフォントや、色の使い方を配慮すること
・用語には、カタカナの利用はなるべく避け、理解しやすいように図や防犯の観点との対比を行うなど配慮すること

(3) 高齢者向け資料の作成指針

外出時リーチ資料および在宅時等リーチ資料の作成指針は、以下のとおりとする。

①外出時リーチ資料の作成指針

- ✓ 目的 ・・・・・・・情報セキュリティに関心を引き起こすきっかけの提供
- ✓ 形式（様式)・・・・1 枚の紙面に 1 メッセージ掲載
- ✓ 形式（媒体)・・・・ポスター
- ✓ 形式（記載分量)・・メッセージ、サポートメッセージ、絵の構成
- ✓ 内容 ・・・・・・・恐怖心を煽らずに、情報セキュリティ対策の必要性を訴求

ポスターは、記載できる分量が限られるものの、情報セキュリティに関心を引き起こすきっかけになるメッセージを伝えることを目的に作成する。普及啓発するメッセージは、情報通信機器の利用シーンの全てを扱うことから、複数枚作成する。

②在宅時等リーチ資料の作成指針

- ✓ 目的 ・・・・・・・情報セキュリティに関してやるべき事、気付くべき内容の提供
- ✓ 形式（様式)・・・・見開き両面
- ✓ 形式（媒体)・・・・リーフレット（A3 版　見開き表裏型）
- ✓ 形式（記載分量)・・見開きにした時に、やるべき事が一覧として理解しやすい記載レイアウト
- ✓ 内容 ・・・・・・・恐怖心を煽らずに、情報セキュリティ対策の必要性を訴求。

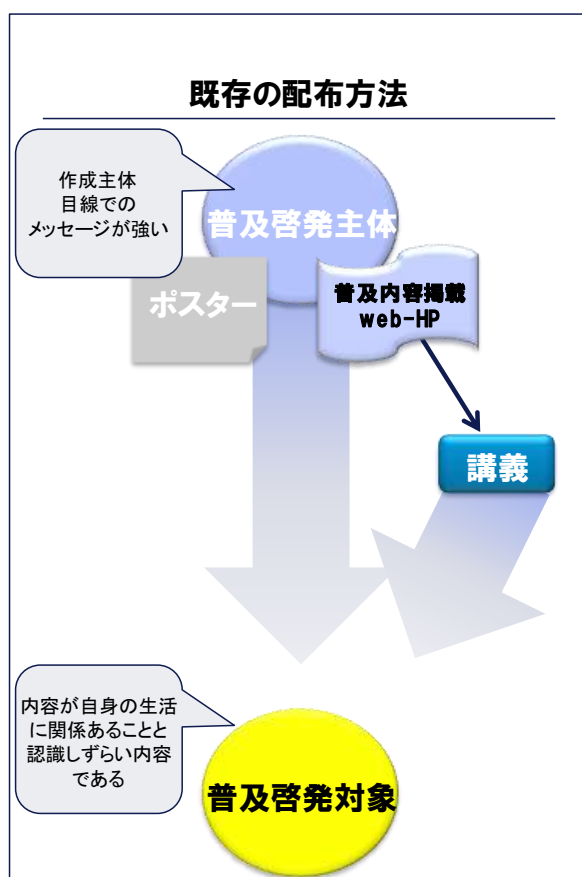
リーフレットは、高齢者が読みやすく理解しやすいことや、高齢者の関心を喚起する観点を重視して、情報通信機器を利活用する際に行うべき、気付くべき情報セキュリティ対策に焦点をあてて作成する。また、リーフレットを自宅で繰り返し確認できるよう、見開いた状態で使えるようレイアウトを配慮する。

3.4. 高齢者向け資料の配布方法

情報セキュリティに関する高齢者向け資料の配布は、既存の取組み事例調査や高齢者が訪問するフィールドの実態を把握し、そこから得られた知見等をまとめて整理する。

(1) 高齢者向け資料における既存の配布方法

事例調査や高齢者が訪問するフィールドの実態の結果、高齢者向け資料は、普及啓発主体がポスターを掲示したり、講義形式での提供が行われていた[39]。併せて、高齢者向けに特化した取組みは、自治体や民間団体等が行っていた[40]。

しかし、既存の配布方法は普及啓発主体の取組みにリーチできるのは、外出が可能なアクティブシニア層に留まる点が懸念される。

図表 40　既存の配布方法

[39] 調査結果は、「別添資料 5　国内事例集」、「別添資料 6　海外事例集」に取りまとめている。
[40] ICT サポーター制度（総務省）、SPREAD サポーター（セキュリティ対策推進協議会）、インターネット安全教室（日本ネットワークセキュリティ協会）、「生・活」知識検討による認定者の講演等活動（東京商工会議所）

(2) 有識者との配布方法に関する検討結果（配布方針）

上記、既存の取組み事例調査の結果、高齢者向け資料の配布方法は、ノンアクティブシニア層の普及啓発対象者に対してもリーチしなければ意味が無い。一方で、リーチするためには、いくらでも予算をかけられるというものでもない。

そこで、普及啓発主体の取組みを前提に、より普及啓発対象へのリーチを高める配布方法を、上記事例調査及び有識者との検討会を踏まえ、ポイントを以下のとおり整理した。

・アクティブシニア層は高齢化に伴い、人数的にも増えてきており、彼らは自身の活躍の場を求めている

・アクティブシニア層を地域社会における高齢者への各種取組みのリーダーとして活用する施策が世の中に既に存在している
  ✧ ICT サポーター制度（総務省）
  ✧ 「生・活」知識検定による認定者の講演等活動（東京商工会議所）
  ✧ SPREAD サポーター（セキュリティ対策推進協議会）
  ✧ インターネット安全教室（JNSA[41]）、等

・地域社会において、高齢者に対する取組みは、一緒に扱うよりも、アクティブシニア層を起点に考え、そこから他の層へ波及させることが有効である

その結果、高齢者向け資料の配布方針として、既存の普及啓発主体の取組みを活かし、いかにアクティブシニア層とノンアクティブシニア層にリーチするかに焦点を当てることとした。

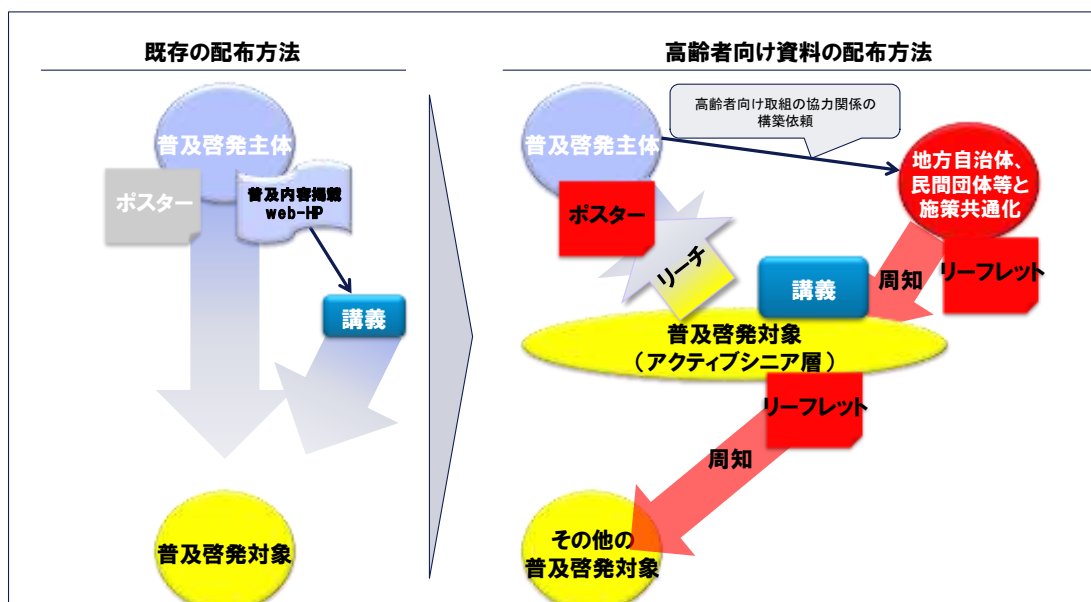
具体的には、普及啓発主体と接点が多いアクティブシニア層をキーとして、既存の取組み組織・団体等との協力関係の下、当取組みの情報を伝えるよう、高齢者向け資料の配布の仕組みを構築することである。

[41] NPO　日本ネットワークセキュリティ協会

(3) 高齢者向け資料の配布方法

本検討では、配布方針を受けて、既存の普及啓発主体の取組みを活かし、普及啓発主体と接点が多いアクティブシニア層をキーとして、既存の取組み組織・団体等との協力関係の下、当取組みの情報をノンアクティブシニア層にも接するよう、高齢者向け資料の配布の仕組みを構築することを提言する。

高齢者を、アクティブシニア層とノンアクティブシニア層に分類したとき、アクティブシニア層は自分の外出先等での居場所や活躍の場を求めていることから、まずはリーチポイントが多いアクティブシニア層に向けた普及啓発施策（ポスター、リーフレット）を普及啓発主体は働き掛けることが有効である。次に、関心を持ったアクティブシニア層は、各自リーフレット等を用いて情報セキュリティリテラシーを向上するとともに、ノンアクティブシニア層へリーフレット等の配布支援を行う等の地域社会における高齢者コミュニティの仕組みの活用を推進する。

いずれにおいても、既存の取組み組織・団体等の協力を仰ぐことが有効である。有識者による検討会においては、アクティブシニア層に対して働きかける場面では地方自治体、民間団体等[42]が、アクティブシニア層がノンアクティブシニア層へ配布支援を行う場面では、東京商工会議所が行っている検定制度[43]などが具体例として示された。

図表 41　既存事例の配布方法と本施策の配布方法

[42] 既存の組織・団体の取組みとしては、ICT サポーター制度や高齢者向け各種普及啓発の取組み（SPREAD）、インターネット安全教室（JNSA）、等がある。

[43] 「生・活」知識検定試験（東京商工会議所）

3.5. 高齢者向け資料（案）

(1) 外出時リーチ資料

本検討の結果は、「別添資料 3　高齢者向け資料（ポスター）」にまとめた。

(2) 在宅時等リーチ資料

本検討の結果は、「別添資料 4　高齢者向け資料（リーフレット）」にまとめた。

4.　考慮事項

　情報セキュリティリテラシー向上のためには、本検討施策以外にも、以下の事項についても考慮すべきであることが、検討を通じて明確になった。

①技術的な取組み
セキュリティ製品・サービス等に係る提供者（ベンダー）側が、情報セキュリティに着目した技術的な取組みの実施。
（例：セキュアなシステム設計）

②インターネット利用時のセキュリティ喚起商品等の充実
セキュリティを喚起する商品・サービスの充実。
（例：インターネット利用時に、セキュリティを喚起する音声を出すおもちゃなど）

③活動原資の仕組みの検討
情報セキュリティ対策を進める上で必要となる原資を作る仕組みの構築。
（例：地上デジタル放送の普及活動や、交通安全運動の取組み、民生委員の制度等を参考とした活動原資の仕組み）

④各施策の定期的見直しの実施
自己診断チェックリストや高齢者向け資料に関する、定期的な記載内容の見直しの仕組みの構築。
（例：最新動向を踏まえた情報セキュリティに係る脅威と対策内容を適宜施策に取り入れるよう、最新化する仕組み）

⑤施策の効果指標、評価の仕組みの検討
本検討を今後も検討する等の参考になる情報セキュリティリテラシーに係る実態調査の実施。

⑥本検討以外の普及啓発対象者への取組み要否の検討
本検討で扱っていない視点（性別分類、年齢別分類、等）の普及啓発対象者への取組み。

情報セキュリティに係る取組みは、ユーザだけが自身のリテラシー向上に取り組むことではなく、ベンダー等の情報通信機器等の提供者や、情報セキュリティに配慮した利用環境、政府による施策の継続的な検討等の総合的な取組みを経て効果を発揮するものと考える。

以上

別添資料1

自己診断チェックリスト（赤版）

情報セキュリティ自己診断チェックリスト
～情報セキュリティ対策　12カ条～

このチェックリストでは、パソコンやスマートフォンなどの機器を利用する場面ごとに、情報セキュリティに関して知るべきこと、やるべきことをまとめました。本チェックリストを用いて、みなさんの情報セキュリティ対策を確認してみましょう。

1. 利用環境の設定
パソコンやスマートフォンには、コンピュータウイルスの感染防止のためのウイルス対策ソフトを導入していますか？

✓

2. パスワードの設定
自分のパソコンやスマートフォンには、他人が容易に推測できないパスワードを起動画面に設定することにより、他人が利用できないようにしていますか？

✓

3. セキュリティの更新
パソコンやスマートフォンのOS(オーエス)※やソフトウェアを更新して常に最新の状態を保っていますか？（※用語解説参照）

✓

4. 紛失したら困る重要情報の取り扱い
紛失したら困る重要情報（電話番号や電子メールアドレス、思い出の旅行写真などの画像データなど）には、パスワードをかけたり、複製（バックアップ）をしていますか？

✓

5. 個人情報の公開範囲の設定
自分や家族、友人の個人情報をSNS(エスエヌエス)※やブログに掲載するときは、情報を伝えたい人にだけ公開するよう、適切に公開範囲を設定していますか？

✓

6. 家族や友人の個人情報の取り扱い
家族や友人の名前やメールアドレス、一緒に撮った写真などをインターネット上に公開するときは、事前に本人の許可を得ていますか？

✓

7. 金融財産情報の取り扱い
金融機関を名乗り、口座番号や暗証番号、クレジットカード情報の入力を促すようなメールがきた場合、安易にそれらの情報を入力しないよう注意していますか？

✓

8. デジタルコンテンツの入手・視聴
スマートフォンのアプリケーション※は、OSを提供している事業者や携帯電話会社などが、安全性の審査を行っている信頼のおける場所から入手していますか？

✓

9. 電子メール利用時
身に覚えのない電子メールには、コンピュータウイルスが潜んでいる可能性があることを認識したうえで、添付ファイルを開かないなどの対応をしていますか？

✓

10. 自宅外利用時
パソコンやスマートフォン、USBメモリなどを持って外出するときは、機器やファイルにパスワードを設定し、なくしたり盗まれたりしないよう気を付けて持ち歩いていますか？

✓

11. トラブル発生時
架空請求の電子メールが大量に届いたり、開いているウェブページをどうしても閉じることができない場合、1人で悩まず誰かに相談していますか？

✓

12. インターネット接続機器利用時
インターネットに接続したテレビやゲーム機器でネットショッピングなどのサービスを利用するときは、ウイルス感染などの脅威に遭う可能性があることを想定して、セキュリティに配慮していますか？

✓

◆用語解説

OS(オーエス)	オペレーティングシステムの略称で、パソコン全体を管理するためのソフトウェアです。具体的には、キーボードの入力やディスプレイ、プリンタへの出力といった入出力機能などの管理を行っています
SNS(エスネヌエス)	SNSとはソーシャルネットワーキングサービスのアルファベットの頭文字をとったもので、個人の日記やフォトアルバムを特定の人に公開できたり、利用者同士が気軽に意見交換できるコミュニティを開設できたりなど、様々な機能を持ったウェブサイトを提供するサービスです
アプリケーション	文書の作成や数値計算など、ある特定の目的のために設計されたソフトウェアです。どのソフトウェアにも共通する基本的な機能をまとめたOSに、ユーザが必要とするものを組みこんで利用します
ワンクリック詐欺	不当な料金請求の手法の1つで、アダルトサイトや出会い系サイトなどにアクセスしたときに、いきなり料金請求の画面が表示されるという手口の詐欺です

◆各種相談窓口

● 購入した製品の具体的な使い方については取扱説明書などに記載されている連絡先へご連絡ください
- ✓各製品の開発元/販売元
- ✓電話番号　各製品の取扱説明書などに記載されています

●コンピュータウイルスに感染してしまったと思ったらこちらにご相談ください
- ✓IPA(アイピーエー)(情報処理推進機構)セキュリティセンター　安心相談窓口
- ✓電話番号　03-5978-7509　(平日10:00～12:00 および 13:30～17:00)

●広告や宣伝目的の迷惑メールに困っている時はこちらへご連絡ください
- ✓財団法人日本データ通信協会　迷惑メール相談センター
- ✓電話番号　03-5974-0068　(平日10：00～17：00)(祝祭日は除く)

●犯罪に係る相談や情報提供を電話で受け付けています
- ✓各都道府県警察のサイバー犯罪窓口
- ✓電話番号　各都道府県警察にお問い合わせください

◆さいごに
みなさんはいくつチェックできましたか？　全てにチェックできるまで繰り返し確認し、安全・安心なデジタルライフを送りましょう。

～解説～

1. 利用環境の設定

パソコンがコンピュータウイルスに感染すると、悪意のある人にパソコンを操られて他のサイトへの攻撃に悪用されたり、プライバシーに係わる大切な情報やクレジットカード番号などの金融情報が漏えいするなどの被害を受ける危険が発生します。

コンピュータウイルスの感染を防ぐために、ウイルス対策ソフトを導入しましょう。（ウイルス対策ソフトは家電量販店などで入手することができます。）

2. パスワードの設定

パソコンやスマートフォンの起動時のパスワードを設定していないと、自分以外の人に機器を利用される危険があります。

自宅に鍵をかけるように、自分だけが利用できるように起動時のパスワードを設定しましょう。パスワードには、住所や電話番号、誕生日のような他人から推測されやすい情報は使用しないようにし、もし、忘れないようにメモに残さざるをえない場合は、人の目に触れない場所にメモを保管するようにしましょう。

3. セキュリティの更新

パソコンやスマートフォンのOSやソフトウェアに存在する情報セキュリティ上の欠陥を“セキュリティホール”と言います。これらにセキュリティホールがあると、たとえウイルス対策ソフトを導入していても、インターネットに接続しただけでコンピュータウイルスに感染してしまうことがあります。

このような被害を防ぐためには、OSやソフトウェアは常に更新し、最新の状態にしておくことが重要です。OSやソフトウェアの更新は自動更新に設定しておくと便利です。

4. 紛失したら困る重要情報の取り扱い

次の情報は、インターネット上にひとたび公開されると、プライバシーを侵害されるなどの精神的な苦痛を受けるかもしれません。

【個人情報】氏名、誕生日、住所、性別、体重、メールアドレス、電話番号、学歴、病歴など
【思い出情報】家族や友人と写った旅行写真や動画、想い出に残る物や景色の写真など

漏えいすると困るファイルなどにはパスワードをかけておくとよいでしょう。

また、消えてしまうと取り返しのつかない思い出情報を含むファイルなどは復元できるようにUSBメモリなどにバックアップを取っておくなどの対策が有効です。

5. 個人情報の公開範囲の設定

SNSやブログでは、個人情報を公開するときに公開する範囲を制限することができますが、それを知らずに利用している人も中にはいます。自分自身のスケジュールや家族や友人と撮った思い出の写真を公開範囲を制限せずに一般公開してしまうと、自分をはじめ、家族や友人も、不特定多数の人からプライバシーを侵害されるかもしれません。

SNSやブログで自分や家族、友人の個人情報を公開するときには、自分が情報を伝えたい人にだけ公開範囲を制限しましょう。

6. 家族や友人の個人情報の取り扱い

自分の個人情報を漏えいしないように取り扱うことは大切ですが、家族や友人の個人情報を知らぬうちに勝手に公開しないなどの配慮も大切です。例えば、家族や友人と一緒に写った写真や動画は、あなたの情報でもあり家族や友人の情報でもあります。あなたの判断で良いと思って公開した情報であっても、家族や友人からしたら公開して欲しくない情報かもしれません。

家族や友人の個人情報をインターネット上に公開するときは、情報を公開しても良いか、本人から事前に許可をもらうようにしましょう。

7. 金融財産情報の取り扱い

金融機関などになりすまして、口座番号や暗証番号、クレジットカード情報などの入力を促すようなメールを送り、財産をだまし取ることを“フィッシング詐欺”と言います。

フィッシング詐欺の被害に遭わないためには、口座の暗証番号などの入力を催促するメールが届いても、覚えのないメールは返信せず、通帳やカードに記載されている金融機関の連絡先に事実確認を行うなど、安易に口座番号や暗証番号などの金融財産情報を伝えないことが大切です。

8. デジタルコンテンツの入手・視聴

インターネット上には映像や動画を入手したり視聴する環境が充実しています。
一方で、悪意ある人がコンピュータウイルスを忍ばせたアプリケーションを提供し、利用者がダウンロードし実行してしまったことで、ウイルスに感染してしまうことがあります。ウイルスによって、パソコンの中にあるファイルやソフトウェアが壊されたり、情報が盗まれたりする被害も発生しています。

上記のような悪意のあるアプリケーションによる被害を回避するために、安全性の審査が行われているサイトからデジタルコンテンツをダウンロードしましょう。

9. 電子メール利用時

知らないアドレスから届く電子メールには、家族や友人からのアドレス変更通知やショッピングサイトからのダイレクトメールだけでなく、架空請求などの悪意のあるメールもあります。

このような電子メールにはウイルスが潜んでいる可能性もあります。ウイルス感染を防ぐためには、身に覚えの無い電子メールの添付ファイルは開かないなど、慎重な行動が大切です。

10. 自宅外利用時

外出先でパソコンやスマートフォンをうっかり紛失したり盗まれたりすると、機器の履歴からネットバンキングやネットショッピングへのアクセスを試みられたり、電話帳に登録している友達に迷惑をかけてしまうかもしれません。

例えば、外出先のお店でパソコンやスマートフォンを利用しているときは、少し席を外すのであれば、盗難を防ぐために機器を持って移動しましょう。また機器が盗難されても中の情報が悪用されないように、起動時のパスワードは設定するようにしましょう。

11. トラブル発生時

インターネット利用に関する被害相談として、ワンクリック詐欺※に遭ったり、架空請求の電子メールが大量に届いたり、開いているウェブページをどうしても閉じることができないというような事例が増えているようです。

このような症状が見られたら、1人で悩まず、誰かに相談しましょう。近所に住むセキュリティに詳しい人に相談したり、症状に応じて各種相談窓口に相談すると、よりスムーズにトラブルに対処できるでしょう。

12. インターネット接続機器利用時

インターネットに接続したテレビやゲーム機（以下、情報家電）には、情報検索やネットショッピングなど、パソコンやスマートフォンと同様のインターネットサービスを利用することができるものもあります。このことは、同時にウイルス感染などの情報セキュリティに関する被害に遭う可能性があることを意味します。

このため、まずは情報家電の取扱説明書に書かれているセキュリティ設定を適切に実施することが大切です。

別添資料2

自己診断チェックリスト（黄版）

自己診断チェックリスト（黄版）

【はじめに】
　この自己診断チェックリストは、自分の情報セキュリティ対策についての知識の正確性・理解度を確認するものです。

　本チェックリストは、インターネットに接続できるパソコンやスマートフォンなどの機器を利用するシーンごとに、理解しておくべき知識、対策、注意事項などをクイズ形式でまとめています。本リストの全問をチェックすることで、自分が何を理解できていて、何を理解できていないのか、理解度を把握することができます。

　本リストを自分自身の情報セキュリティの向上にお役立て下さい。

0. 自己診断チェックリストについて

この自己診断チェックリストは、全22問の3択クイズです。
解答は、下にある解答欄に記入しましょう。縦には選択肢、横にはクイズ番号が並んでいます。各問の選択肢の文字に○を付けていくと、全部解き終わったときには、2つのメッセージが浮かび上がってきます。
早速問題にチャレンジして、メッセージを解読しましょう！！

【解答欄】

メッセージ1

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
A1	あ	た	よ	せ	な	み	ゆ	え	て	か	ご
A2	き	も	し	い	な	ゆ	き	り	い	い	う
A3	ら	ん	み	ん	せ	き	く	か	と	じ	ー

守って ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ！！

メッセージ2

	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22
A1	う	の	よ	は	い	ろ	た	る	あ	て	と
A2	た	り	し	い	ず	ひ	か	み	か	つ	も
A3	え	お	こ	じ	み	ん	し	ー	ね	や	み

使って ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ！！

1.　利用環境の設定

Q1/22

新しく購入したパソコンやスマートフォンの利用環境設定時に、情報セキュリティ対策として行うべき対応のうち、最も適切な選択肢はどれでしょうか？

A1　ウイルス対策ソフトを導入する他、起動画面にもパスワード設定を行う

A2　ウイルス対策ソフトは導入せず、起動画面にパスワードを設定する

A3　信頼できる製造メーカーの製品を購入しているため、特に対策は必要ない

2.　起動時のセキュリティ対策

パスワードを他人から推測されにくくする工夫として最も適切な選択肢はどれでしょうか？

A1　自分と特定の友人しか知り得ない合言葉をパスワードにする

A2　個人の主観がパスワードに反映されないように、複数の友人と知恵を出し合って、複雑なパスワードを作る

A3　文字だけでなく数字や記号を織り交ぜてパスワードを作る

3.　セキュリティの更新

Q3/22 **パソコンやスマートフォンに導入されているOS(オーエス)※に情報セキュリティ上の欠陥が見つかりました。その情報セキュリティ対策として行うべき行動のうち、最も適切な選択肢はどれでしょうか？**

A1　ウイルス対策ソフトの更新を止める

A2　OSの修正プログラム(セキュリティパッチ)を適用する

A3　情報セキュリティ上の欠陥を放置していても、インターネットの利用には問題ない

> ※OS：オペレーティングシステムの略称で、パソコン全体を管理するためのソフトウェアです。具体的には、キーボードからの入力やディスプレイ、プリンタへの出力といった入出力機能などの管理を行っています。

Q4/22 **パソコンやスマートフォンのOSやソフトウェアに発見された情報セキュリティ上の欠陥を修正せずに放置した場合に考えられる状況は、どの選択肢でしょうか？**

A1　ウイルス対策ソフトを導入していれば、情報セキュリティ上の欠陥を修正しなくてもウイルスに感染することはない

A2　OSやソフトウェアに見られる情報セキュリティ上の欠陥は、対策を打たなくても時間の経過とともに自然と修復される

A3　ウイルス感染の危険性が増大する

4.　個人情報の取り扱い

Q5/22 **自分や家族・友人の個人情報※が、インターネット上に漏えいしたときに考えられる状況として間違っている選択肢はどれでしょうか？**

A1　自分の不注意で、家族や友人のプライバシーが侵害される可能性が発生する

A2　自分のプライバシーが侵害される可能性が発生する

A3　誰も全く被害を受けることはない

> ※個人情報：氏名、誕生日、住所、メールアドレス、電話番号、血液型、国籍、学歴など

Q6/22 **自分や家族・友人の個人情報が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1　多くの危険を伴うファイル共有ソフト※は利用しない

A2　安易に、プライバシーに関わる個人情報はインターネット上に公開しない

A3　個人情報は、できるだけたくさんのUSBメモリやCD-Rなどに複製(バックアップ)する

> ※ファイル共有ソフト：不特定多数のコンピュータ間でファイルの共有や交換を行うソフトウェア。Winny,share,Cabosなどがある

5. 金融・財産情報の取り扱い

Q7/22 **金融・財産情報※が、インターネット上に漏えいした場合に考えられる状況として間違っている選択肢はどれでしょうか？**

A1 取引銀行のネットバンキングのログインパスワードが漏えいしても、銀行のキャッシュカードを紛失していなければ、不正に取引されることはない

A2 ネットバンキング用のログインパスワードが勝手に変更される

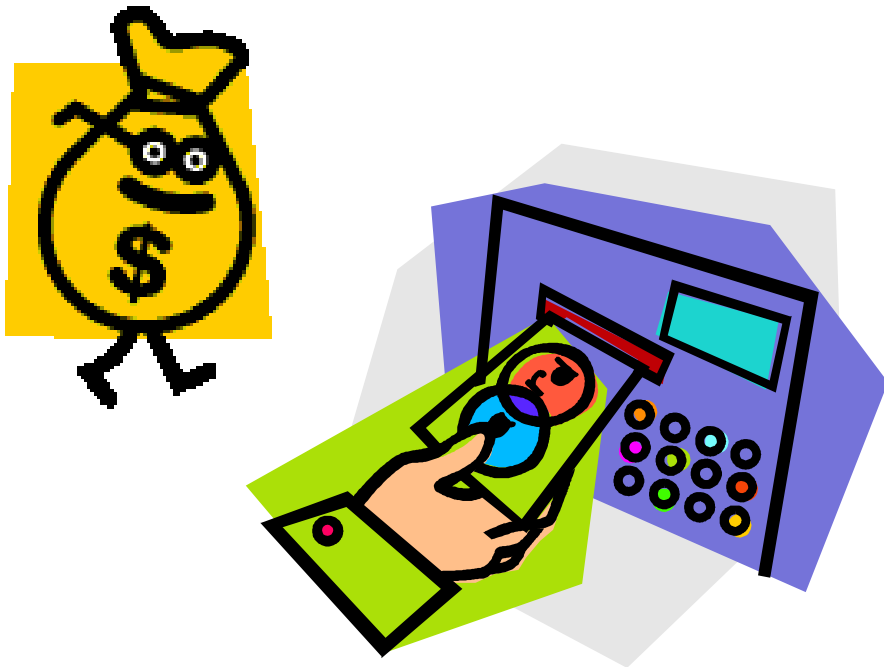
A3 自分の口座から知らぬ間に、他人に振込がされている

※金融・財産情報：口座番号・暗証番号、ネットバンキング用のログインパスワード、クレジットカード番号など

Q8/22 **金融・財産情報が、他人から盗み取られないように、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1 ネットバンキングを利用した後は、入力した履歴を削除するよう心がけている

A2 ネットバンキング用のログインパスワードは、忘れると困るので、生年月日や、同じ数字を連続したものを使い続けることにしている

A3 金融機関を名乗り、口座番号やクレジットカードの有効期限、暗証番号の入力を促すメールが届いたとき、安易にそれらの情報を入力しないよう注意している

6. 思い出情報の取り扱い

Q9/22 **パソコンやスマートフォンに保存されている思い出情報※が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1 ファイル共有ソフトを用い、不特定多数のコンピュータ間で様々なファイルを共有する

A2 セキュリティ対策ソフトを導入する

A3 漏えいして困るファイルにはパスワードをかけておく

※思い出情報：思い出に残る大切な写真や動画（家族や友人と一緒に写った写真・動画、など）

Q10/22 **家族や友人と写った写真や動画をインターネット上に公開するときの行動として、間違っている選択肢はどれでしょうか？**

A1 インターネット上に公開する写真などに写っている家族や友人から、その写真や動画を公開することの許可を得る

A2 きれいに撮れた写真なので、インターネット上にすぐに公開する

A3 ブログなどの日記に掲載する写真は、公開しても困らないようなものを選択して掲載する

7. 紛失したら困る重要情報の取り扱い

Q11/22 **パソコンなどが故障した場合に、そこに保存している重要な情報（思い出情報など）を失わないように、日頃から注意すべき行動のうち、もっとも適切な選択肢はどれでしょうか？**

A1 同じパソコンの別のフォルダにもう一つ複製（バックアップ）している

A2 故障に対するメーカーの有償修理サポートを切らさないよう注意している

A3 日頃からパソコンなどの機器が故障することに備えて、失いたくない重要な情報はUSBメモリ・外付けハードディスク・DVD-Rなどに複製（バックアップ）しておく

8. デジタルコンテンツの閲覧、入手

Q12/22 **ホームページ（ウェブ）を閲覧する時に、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1 画像やリンクをクリックしたときに、意図しない入会完了画面や料金請求画面が表示されたときには、消費生活センターや警察などに相談する

A2 画像やリンクをクリックしたときに、意図しない入会完了画面や料金請求画面が表示されたときには、画面に表示されている問合せ先に電話や電子メールで連絡し、入会を取り消して欲しい旨を伝える

A3 閲覧しようとするURLは、信頼できるホームページかどうか、「ホームページの信頼性評価」などの機能がついているウイルス対策ソフトを使って判断するようにしている

Q13/22 **デジタルコンテンツ※の入手（ダウンロード）に際して、注意することとして間違っている選択肢はどれでしょうか？**

A1 気になるファイルは全てとりあえずダウンロードして、後でファイルに保存されている情報を確認するようにする

A2 ファイルの提供元の名前や事業内容を確認してからダウンロードを行う

A3 ウイルス対策ソフトのパターンファイルを最新の状態に保っていることを確認したうえで、ファイルにウイルスチェックをかける

※デジタルコンテンツ：音楽、音声、映像、ゲームソフトなど

9. 電子メール利用時の注意事項

Q14/22 **電子メールの受信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？**

A1 知らないアドレスから届く電子メールに添付されているファイルは、安易に開かないように注意する

A2 電子メールの送信元のアドレスに覚えのないときには、返信して相手の名前や自分との関係を聞く

A3 覚えのないアドレスから届く電子メールは、友人や知人からのアドレス変更通知以外に、悪意のあるメールが含まれているかもしれないと考える

Q15/22 **電子メールの送信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？**

A1 携帯電話のアドレス変更通知を電子メールで一括送信するときには、それらのアドレスが送信先間に公開されないようにBcc(ビーシーシー)で送信する

A2 他人に電子メールを転送するような指示のあるメールを受信したら、なるべく早く多くの友人に電子メールを転送する

A3 誤送信の危険を減らすため、送信アドレスの入力後に再度、正しく入力されているか確認することにしている

10. ネットワークを介したゲームや情報家電の利用

Q16/22 **インターネットに接続してゲーム機器を利用するときに、情報セキュリティに関して意識しておくべき状況として間違っている選択肢はどれでしょうか？**

A1 パソコンやスマートフォンとは異なり、ゲーム機器はインターネットに接続して利用してもウイルスに感染することはない

A2 パソコンやスマートフォンと同じようにゲーム機器もウイルスに感染することがある

A3 パソコンやスマートフォンと同じようにゲーム機器もインターネットに繋がっているので、個人情報の取扱には注意が必要である

Q17/22 **インターネットに接続してゲーム機器や、デジタルテレビなどの情報家電を利用するときに、情報セキュリティ対策として意識しておくべき対応のうち、間違っている選択肢はどれでしょうか？**

A1 製造元から公開される修正プログラム(セキュリティパッチ)が公開された場合は、自動更新あるいはすぐに修正プログラムを適用する

A2 パソコンからインターネットを利用する時と同様に、パスワードは自分だけの秘密にする

A3 機器の取扱説明書に記載された設定を行ったので、それ以上特に利用時に意識しておくことはない

11. SNSやブログ利用時の注意事項

Q18/22 **SNS(エスネヌエス)※やブログの利用に関して、情報セキュリティの観点から間違っている選択肢はどれでしょうか？**

A1 SNSやブログで知り合った人との交流を広げるためにも、自分のプライバシー情報は積極的に公開して、相手から信頼を受けるようにしている

A2 友人を名乗る不審なメッセージが届いたときは、本人から直接得ている連絡先に事実確認を行うよう配慮している

A3 ブログなどの日記に掲載する写真は、公開しても誰も困らない写真を選択して掲載する

※SNS：ソーシャルネットワーキングサービスのアルファベットの頭文字をとったもので、個人の日記やフォトアルバムを特定の人に公開できたり、自分とSNS参加者が気軽に意見交換できるコミュニティを開設できたりなど、様々な機能を持った自分専用のウェブサイトです。

Q19/22 **スマートフォンを通じてSNSやブログに情報を公開することに関して間違っている選択肢はどれでしょうか？**

A1 スマートフォンで撮影した写真には、位置情報が記録されている場合もあるので、居場所の情報が知られたくない場合は、位置情報の設定を加工して知られないよう取り扱うことにしている

A2 SNSやブログのプロフィールで公開する情報は、誰に見られてもいいように取捨選択している

A3 街中でスマートフォンで撮影した写真に他人が写っている場合、自分とは関係のない人なので、特に配慮することなく公開しても問題はない

１２.　自宅外利用時

Q20/22 **紛失したら困る重要な情報が保存されたパソコンやスマートフォン、USBメモリ※などを持って外出するとき、情報セキュリティ対策上、注意すべきこととして間違っている選択肢はどれでしょうか？**

A1 機器の紛失や盗難を防ぐために、貴重品を扱うのと同様に、常に所在を意識した行動をする

A2 USBメモリの中のファイルにパスワードを設定しておく

A3 重要な情報を持っていることを周囲に気づかれないよう、持っていることを忘れて、平常通りの行動をする

※USBメモリ：持ち出し持ち運び可能な記憶装置です。

Q21/22 **外出先で無線LANに接続してインターネットを利用する場合のセキュリティに関する注意として間違っている選択肢はどれでしょうか？**

A1 パソコンのファイアウォール機能を有効にしておく

A2 電波を利用した通信形態をとる無線LANは盗聴される心配はない

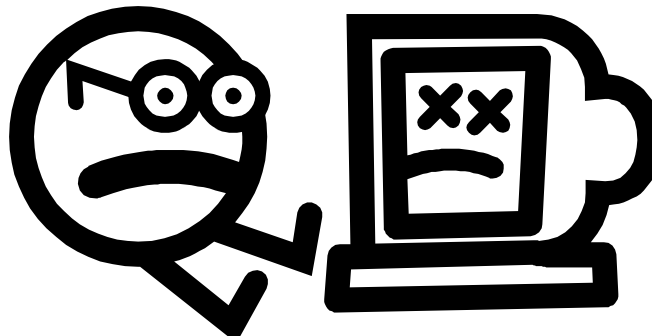
A3 漏えいして困るような情報のやりとりや、金融取引を行わないようにしている

１３.　トラブル発生時の対応

Q22/22 **インターネット利用時にコンピュータのセキュリティに何か異常を感じたとき(例えば、架空請求のメールが届いたり、開いているページを閉じることができないなど)の対応として間違っている選択肢はどれでしょうか？**

A1 数か月様子を見て、それでも異常を感じるようだったら、誰かに相談する

A2 有線回線を利用している場合は、すぐに回線を抜く

A3 困ったときは1人で悩まず、すぐに誰かに相談する

自己診断チェックリスト　黄版

解答・解説

1.　利用環境の設定

Q1/22　**新しく購入したパソコンやスマートフォンの利用環境設定時に、情報セキュリティ対策として行うべき対応のうち、最も適切な選択肢はどれでしょうか？**

【解答】
A1．ウイルス対策ソフトを導入する他、起動画面にもパスワード設定を行う

【解説】
　購入したばかりのパソコンやスマートフォンは、すぐにインターネットが利用できるようにアプリケーションの設定に取り掛かりたい気持ちに駆られます。
　しかし、インターネットの利便性を享受するためには、安心安全なセキュリティ環境の確保が不可欠です。インターネット上には、パソコンやスマートフォンに悪さ※をするコンピュータウイルスなどが存在します。利用する前には、ウイルス対策ソフトを導入したり、自分以外の人に勝手に機器を利用されないよう起動画面にパスワードを設定しましょう。
よってA1が適切です。

　A2は、利用環境として自分以外の人がパソコンを使用することを防ぐだけであり、情報セキュリティ対策であるウイルス対策ソフトを導入していないので、不適切です。
　A3は、信頼できるメーカーの製品だとしても、コンピュータウイルスは技術の隙間を突いたり、進化したりする特徴があります。このため、どのメーカーの製品だとしても、セキュリティ対策は必要です。

※悪さとは、パソコンなどの機器を壊したり、機器の中の個人情報や金融・財産情報を盗み取ったり、改ざんしたり、インターネット上に勝手に公開したりするものです。その結果利用者は精神的・金銭的苦痛を受けてしまいます。

2.　起動時のセキュリティ対策

パスワードを他人から推測されにくくする工夫として最も適切な選択肢はどれでしょうか？

【解答】
A3．文字だけでなく数字や記号を織り交ぜてパスワードを作る

【解説】
　パスワードを起動画面に設定していないと、自分のパソコンやスマートフォン、ゲーム機器を自分以外の人に使われてしまい、中の情報を見られたり、消されたりする危険があります。
そこで、他人に使われないために、起動画面にパスワードを設定することが重要です。

　ただし、パスワードを設定しても、そのパスワードを自分以外の人がすぐに分かってしまっては意味がありません。より強いパスワードを作るためには以下のような注意が必要です。
・数字や記号、大文字、小文字を組み合わせる
・文字数を増やす（長ければ長いほどパスワードは強くなります
・氏名や住所、電話番号、車のナンバープレートのような推測しやすいパスワードは避ける

　さらに、パスワードは自分だけで管理することが大切です。選択肢A1やA2は、友人や知人にパスワードを知られていることになるので不適切です。
　同じ理由で、パスワードを忘れないようメモに残す場合でも、人目に触れる場所に貼ったりするのではなく、貴重品の保管場所と同じ場所に保管するなど、自分だけの秘密として管理しましょう。

3.　セキュリティの更新

Q3/22

パソコンやスマートフォンに導入されているOS(オーエス)※に情報セキュリティ上の欠陥が見つかりました。その情報セキュリティ対策として行うべき行動のうち、最も適切な選択肢はどれでしょうか？

【解答】
A2. OSの修正プログラム(セキュリティパッチ)を適用する

【解説】
　コンピュータに悪さをするコンピュータウイルスやスパイウェア※１、ボット※２などの不正プログラムの中には、パソコンやスマートフォンに存在する情報セキュリティ上の欠陥（セキュリティホール）を狙ってくるものもあります。これらの機器にセキュリティホールがあると、インターネットに接続しただけでコンピュータウイルスに感染してしまうこともあります。
　製造元は、このようなセキュリティホールを発見しては、セキュリティパッチと呼ばれる修正プログラムを公開しているので、セキュリティホールを修正するために、常に最新のものを適用（アップデート）しましょう。よってＡ２が適切です。

Ａ１、Ａ３は、情報セキュリティ上の欠陥に対応していないため、ウイルスに感染しやすくなり、インターネットの利用に支障を来たす可能性があります。したがって、A1、A3ともに適切ではありません。

※１スパイウェア：スパイウェアは、情報を収集する不正プログラムであり、コンピュータに保存されている情報を収集し、悪意ある第三者に送信することを目的としています。

※２ボット：ボットとは、コンピュータを外部から操る不正プログラムです。感染すると、他のコンピュータに対して不正プログラムをばらまくなど、加害者の手先として操られてしまいます。ボットに感染したコンピュータは、被害者であると同時に、加害者になってしまうのが特徴です。

パソコンやスマートフォンのOSやソフトウェアに発見された情報セキュリティ上の欠陥を修正せずに放置した場合に考えられる状況は、どの選択肢でしょうか？

【解答】
A3. ウイルス感染の危険性が増大する

【解説】
　パソコンやスマートフォンにセキュリティホールがあると、インターネットに接続しただけでコンピュータウイルスに感染してしまうこともあります。ＯＳやソフトウェアのアップデートを行ってセキュリティホールを修正しないと（Q3解説参照)、セキュリティホールを狙う新たなウイルス感染などに繋がります。よってA３は考えられる状況です。

　Ａ１は、たとえウイルス対策ソフトを導入していたとしても、セキュリティホールがあると、ウイルスに感染してしまうこともあるので間違いです。Ａ２は、OSやソフトウェアのアップデートなどの対策を打たなくとも、セキュリティ上の欠陥が自然に修復されることはないため間違いです。

4.　個人情報の取り扱い

Q5/22 **自分や家族・友人の個人情報が、インターネット上に漏えいしたときに考えられる状況として間違っている選択肢はどれでしょうか？**

【解答】
A3. 誰も全く被害を受けることはない

【解説】
電子データはその性質上、簡単にデータを複製して流通させることができるため、個人情報がひとたび漏えいすると、完全に回収することが困難です。情報が漏えいすると自分のプライバシーがインターネット上の複数のサイトに転載されたり、情報に家族や友人の個人情報が含まれている場合は、自分だけでなく家族や友人にも影響が及んだりする場合があります。よってA1、A2は正しい状況です。
このため、「誰も全く被害を受けることはない」というA3が間違っている状況を示す選択肢です。
なお、個人情報には、以下のような項目が該当します。

- 氏名
- 生年月日
- 性別
- 血液型
- 身長
- 体重
- 身体特性
- 個人の写真
- 生体認証情報
- 人種
- 国籍
- 住所
- メールアドレス
- 電話番号
- パスポート情報
- 学歴系情報
- 勤務履歴情報
- 健康保険証情報
- 年金証書情報
- 免許番号
- 介護保険証情報
- 健康診断結果
- 趣味・嗜好
- その他プライバシー情報（犯罪歴・政治思想など）
- 家族・友人・知人の個人情報

など

個人情報は、自分自身の情報だけではなく、家族や友人などの情報も守るように意識しましょう。

自分や家族・友人の個人情報が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】
A3. 個人情報は、できるだけたくさんのUSBメモリやCD-Rなどに複製(バックアップ)する

【解説】
A1は、ファイル共有ソフトの利用についての選択肢です。ファイル共有ソフトは、不特定多数のコンピュータ間でファイルの共有や交換を行うソフトウェアなので、利用者のミスや設定の誤りによって、公開したくないファイルを公開してしまうなど、利用には危険が伴います。Ａ１は正しい行動です。

プライバシーに関わる情報は公開前に公開する範囲（誰にどんな情報を公開するか）を判断しましょう。公開範囲を制限しないと、見知らぬ人にも自分のプライバシー情報を公開することになり、トラブルの原因になります。よってA2は正しい行動です。
Ａ３は、漏えいしないための対策ではありません。よってA3は間違っている行動です。

5. 金融・財産情報の取り扱い

金融･財産情報が、インターネット上に漏えいした場合に考えられる状況として間違っている選択肢はどれでしょうか？

【解答】

A1. 取引銀行のネットバンキングのログインパスワードが漏えいしても、銀行のキャッシュカードを紛失していなければ、不正に取引されることはない

【解説】

金融・財産情報には以下のようなものがあります。

- 所得情報（年収・借入金・残高情報など）
- 口座番号・暗証番号
- クレジットカード番号
- 印鑑登録証明書
- 金融機関のログインアカウント
- 所有不動産情報（所在地・資産取得価額、借入情報など）
- その他、不動産情報
  （有価証券・社債・国債など）

上記のような情報が悪意のある人に知られてしまうと、自分の知らないうちにネットバンキングで利用されるなど、自分の金融財産を不正に利用される状況が考えられます。
そのような被害を防ぐために、クレジットカードや銀行口座の利用明細を確認し、身に覚えの無い取引があった場合は金融機関に連絡して利用を中止するなどの対応が必要です。
取引銀行のネットバンキング用のログインパスワードが漏えいした場合は、銀行のキャッシュカードを紛失していなくても不正に取引を行われる可能性があるので、Ａ１は間違いです。また、ログインパスワードが漏えいすると、第三者がログインパスワードを勝手に変更したり、他人の口座へとお金を振り込んだりすることも可能になります。よって、A2、A3は考えられる状況です。

【参考】

悪意のある人がこれらの情報を手に入れるのに使う代表的な手口として、フィッシングやソーシャルエンジニアリングがあります。

フィッシング：
巧妙な文面のメールなどを用いて、実在する金融機関などを装い、個人情報や金融・財産情報の入力画面に誘導して、暗証番号やクレジットカード番号などを盗み取る不正行為

ソーシャルエンジニアリング：
ネットワークシステムへの不正侵入を行うために、コンピュータ技術などを利用するのではなく、人の心理面に付け込んだ手段（話術や盗み聞き、盗み見などの「社会的」な手段）によって、パスワードなどのセキュリティ上重要な情報を入手すること

フィッシングは、ユーザを騙すことによって成り立つ不正行為であるため、怪しいメール、リンク先などを疑ってかかるなどの用心深い意識行動が対策として重要です。正規のサイトと偽造されたサイトを区別するのは困難なため、まずは、心当たりのないメールの誘導に対して暗証番号やクレジット番号を安易に入力しないよう、注意を払うことが大切です。
ソーシャルエンジニアリングは、ゴミの中から目的の情報を収集する方法、パソコン画面の覗き見や電話の盗み聞きなどによって情報を収集する方法、他人になりすまして情報を聞き出す方法などがあります。ソーシャルエンジニアリングへの対策としては、機密情報はシュレッダーにかけたり、パソコンやスマートフォンの画面にプライバシーフィルターを貼ったり、少しでも不審に感じた電話には応じないなどの方法があります。

Q8/22 金融・財産情報が、他人から盗み取られないように、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】

A2. ネットバンキング用のログインパスワードは、忘れると困るので、生年月日や同じ数字を連続したものを使い続けることにしている

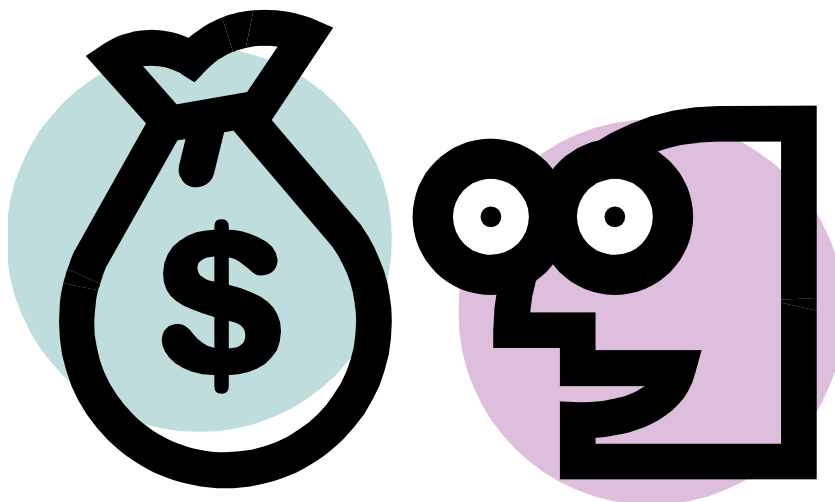
【解説】

パスワードは他人に推測されにくいものとし、定期的に変更するなど、他人に知られないよう管理することが必要です。Ａ２のように、他人から推測されやすいパスワードを変更せずに使い続けると、他人に知られる危険性が高まります。よってA2は間違った選択肢です。

パスワードは、ネットバンキングなどを利用した後は、パソコン上に記録が残っている場合もあるので、入力した履歴を削除するよう、心がけることが大切です。よってＡ１は正しい行動です。

また、Ａ3のようなメールもあるので、大切な情報をだまし取られないよう注意した行動をとりましょう。

【参考】

最近、インターネット喫茶などの共用利用できる機器の中には、「キーロガー」と呼ばれる悪質なソフトウエアに感染しているものもあり、機器に入力したキー操作を盗み取られることがあります。実際にインターネット喫茶からのインターネットショッピングでは、入力したクレジットカード番号や暗証番号が盗み取られた事例もあるので、共同利用できる機器での金融・財産情報の取り扱いには注意が必要です。

6.　思い出情報の取り扱い

Q9/22

パソコンやスマートフォンに保存されている思い出情報が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】
A1. ファイル共有ソフトを用い、不特定多数のコンピュータ間で様々なファイルを共有する

【解説】
　思い出情報には、家族や友人との旅行写真や動画、日記、また思い出に残った景色などの写真や動画などが含まれます。
　家族や友人と一緒に写った写真や動画は、自分だけではなく、一緒に写った家族や友人にとっても大切な情報です。そのため、それらの写真が漏えいした場合、自分や家族、友人のプライバシーが侵害されるおそれがあります。このような被害を予防するために、セキュリティソフトを導入したり、漏えいして困るファイルにパスワードを設定することは、有効な対策です。よって、A2、A3は適切な行動です。

　ファイル共有ソフトを用いて不特定多数とファイルの共有や交換を行うと、利用者のミスや設定の誤り、ウイルス感染などによる漏えいの危険が高まります。よってＡ１は間違いです。

Q10/22

家族や友人と写った写真や動画をインターネット上に公開するときの行動として、間違っている選択肢はどれでしょうか？

【解答】
A2. きれいに撮れた写真なので、インターネット上にすぐに公開する

【解説】
　自分や家族、友人のプライバシーに係わる情報を公開する時には、本人に許可を取ることがマナーです。人によっては公開を快く思わない人もいるので、許可が得られないときは、インターネットでは公開しないことがトラブル防止に有効です。よってＡ１は正しい行動です。
　また、ひとたび公開するとそれらのデータが様々なサイトに転載され回収が難しくなることもあるので、公開しても困らないものを選択することが重要です。よってＡ３は正しい行動です。
　本人の許可を取ること無く、すぐに公開することは、マナー違反であるばかりでなく、本人とのトラブルの原因になりかねません。よってＡ２は間違った行動です。

7. 紛失したら困る重要情報の取り扱い

Q11/22 パソコンなどが故障した場合に、そこに保存している重要な情報（思い出情報など）を失わないように、日頃から注意すべき行動のうち、もっとも適切な選択肢はどれでしょうか？

【解答】

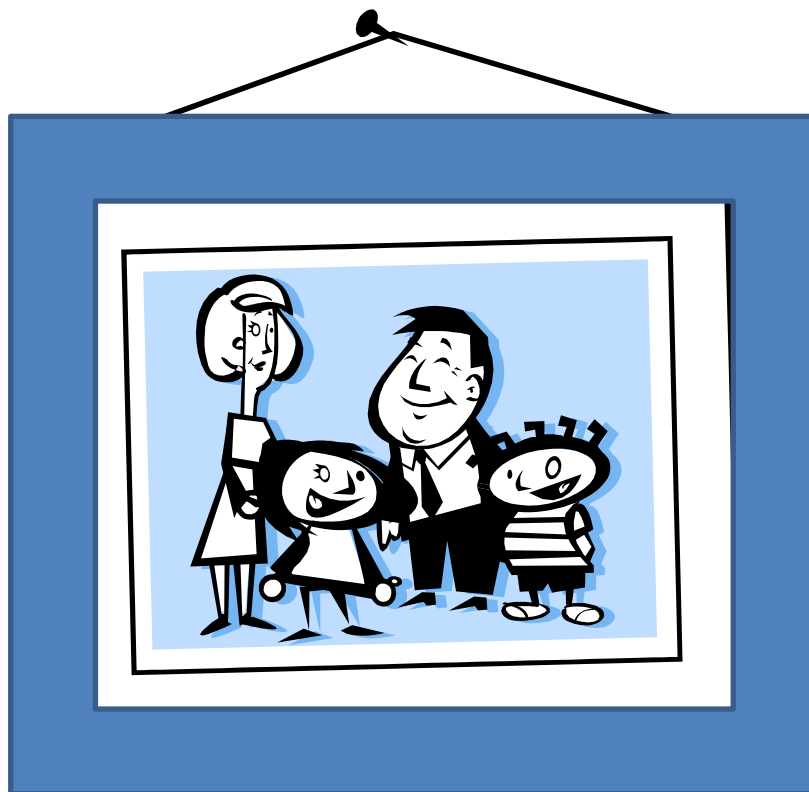
A3. 日頃から、パソコンなどの機器が故障することに備えて、失いたくない重要な情報はUSBメモリ・外付けハードディスク・DVD-Rなどに複製（バックアップ）しておく

【解説】

パソコン上に保存している情報は、パソコンが故障した場合、失われることが想定されます。

そこで、失いたくない重要な情報は、予め複製（バックアップ）を取得しておくことが日頃の備えとして有効です。よってＡ３が適切な行動です

Ａ１は、保存場所が適切ではありません。同じパソコン内に複製すると、パソコンが故障した場合に取り出せなくなります。

Ａ２は、故障自体の修繕には、メーカーサポートは有効ですが、有償サポートの場合でも、多くの場合、パソコンの中のデータまでは保証してくれません。よってＡ２は適切ではありません。

８．　デジタルコンテンツの閲覧・入手

Q12/22 ホームページ（ウェブ）を閲覧する時に、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】
A2. 画像やリンクをクリックしたときに、意図しない入会完了画面や料金請求画面が表示されたときには、画面に表示されている問合せ先に電話や電子メールで連絡し、入会を取り消して欲しい旨を伝える

【解説】
　Ａ１は適切な行動です。トラブルが発生した場合は、一人で悩まずに、身近な人や各種相談窓口に相談しましょう。
　Ａ３のように、ウイルス対策ソフトのなかには、閲覧しようとするＵＲＬが信頼できるかどうかを表示する機能を持つものもあります。このような機能を活用して、ウイルス感染を避けながらホームページ(ウェブ)閲覧を楽しみましょう。よってA3は適切な行動です。

　URLをクリックしただけで、意図しない入会完了画面や料金請求画面が表示され、それを信用してお金を振り込んでしまう被害は“ワンクリック詐欺”と呼ばれています。これらの画面が表示されたら、無視することが適切な対策の1つです。架空の請求画面に表示されている問合せ先に連絡してしまうと、連絡に使った電話番号やメールアドレスにも請求がくるようになり、事態が悪化することもあるので、Ａ２の対応は適切ではありません。

Q13/22 デジタルコンテンツの入手（ダウンロード）に際して、注意することとして間違っている選択肢はどれでしょうか？

【解答】
A1. 気になるファイルは全てとりあえずダウンロードして、後でファイルに保存されている情報を確認するようにする

【解説】
　インターネットには悪意のある人も存在します。悪意のある人が提供するファイルにはウイルスが含まれている危険があります。そのため、ファイルをダウンロードするときに提供者の名前や事業内容をインターネットで確認するなど、信頼できる相手かどうか判断することが大切です。よってA2は適切な行動です。

　また、インターネットでダウンロードできるファイルには新種のウイルスを含むものもあります。セキュリティソフトの有効期限が切れたまま、安易にファイルをダウンロードすると、新種のウイルスに感染する危険が高まります。Ａ３に示すようにウイルス対策ソフトは最新のものに更新し、新種のウイルス感染への対策を行いましょう。

　A1のように、気になるからといって安易にダウンロードするのは情報セキュリティ上望ましくありません。ウイルスを含んだファイルがパソコンに侵入しないように慎重な行動を心がけましょう。よって、A1は適切な対応ではありません。

９．　電子メール利用時の注意事項

Q14/22 電子メールの受信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？

【解答】

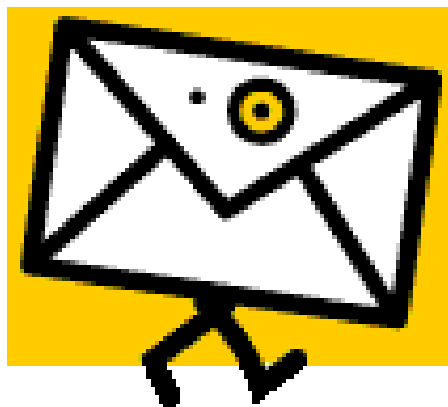
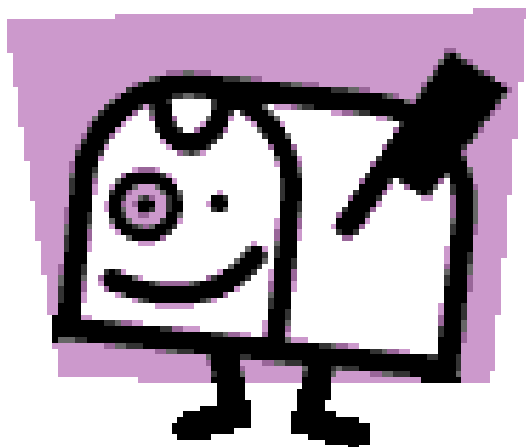
A2. 電子メールの送信元のアドレスに覚えのないときには、返信して相手の名前や自分との関係を聞く

【解説】

知らないアドレスから電子メールが届いたときは注意を払う必要があります。知らないアドレスからメールが届く場合の例として以下のような場合が考えられます。よってＡ3は適切です。

・家族や友人からのアドレス変更通知
・家族や友人に紹介された知人から届く初めてのメール
・コンビニやレンタルビデオ店のサービス紹介メール
・架空請求メールやウイルスを媒介するメール　など

添付ファイルにはウイルスが含まれている可能性もありますので、Ａ1のように安易に添付ファイルを開かないようにしましょう。Ａ1は適切です。

返信して名前や自分との関係を聞くのは危険です。返信することでよりたくさんの迷惑メールが届くようになったりするので、安易に返信はしないようにしましょう。よってＡ2は不適切です。

Q15/22 電子メールの送信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？

【解答】

A2. 他人に電子メール転送するような指示のあるメールを受信したら、なるべく早く多くの友人に電子メールを転送する

【解説】

Ａ２のような電子メールをチェーンメールといいます。このメールの特徴は、電子メールを多くの人に送信させるというものです。このような電子メールが届いた場合は、転送しないでそのまま削除するようにしましょう。チェーンメールを転送してしまうと、ネズミ算式にメールが増加するため、ネットワークやメールサーバーに負荷がかかり、通信速度が遅くなるなどの影響が多くの人に及ぶ可能性があります。よって、Ａ２は間違った選択肢です。

メールを送信するときには、To(トゥー)、Cc(シーシー)、Bcc（ビーシーシー）の3つの宛先指定方法を使い分けることが重要になってきます。

・To・・・・メールの宛先となる相手のアドレスを入れます。そのメールを受信した人全員が、Toに指定されたアドレスを見ることができます。

・Cc・・・・「Toに宛てたメール」のコピーを送る相手のアドレスを入れます。Toと同様に、そのメールを受信した人全員が、Ccに指定されたアドレスを見ることができます。

・Bcc・・・・用途はCcと同じですが、Bccに指定されたアドレスは、そのメールを受信した人に見られることはありません。

携帯電話やスマートフォンのメールアドレスを変更し、その連絡をするときなど、お互いがメールアドレスを知らない複数の人に一斉にメールを送りたいときに、Bccを使用します。よってＡ1は適切です。

また、Ａ３のように、誤送信を防ぐためには、送信アドレスに入力した内容は、送信する前に再度正しいアドレスが入力されているか確認したうえで送信しましょう。よってＡ3は適切です。

１０．ネットワークを介したゲームや家電機能の利用

Q16/22 インターネットに接続してゲーム機器を利用するときに、情報セキュリティに関して意識しておくべき状況として間違っている選択肢はどれでしょうか？

【解答】

A1. パソコンやスマートフォンとは異なり、ゲーム機器はインターネットに接続して利用してもウイルスに感染することはない

【解説】

インターネットに接続してゲーム機器を利用するときは、それが単なるゲームではなく、パソコンやスマートフォンを使ってインターネットに接続している環境と類似していることを意識しておくことが重要です。ゲーム機器がウイルスに感染することも考えられます。よってA1は間違いであり、A2は適切です。

また、ゲーム機器がインターネットに繋がっていることを意識して、「４．個人情報の取り扱い」「５．金融・財産情報の取り扱い」でとりあげたような被害を受けないよう、注意を払って行動することが必要です。よってA3は適切です。

【参考】

家庭用ゲーム機器は、ネットワークの接続も行えるなど、ゲーム以外の用途において多機能化が進んでいるため、近い将来、コンピュータウイルス感染や不正アクセス、金銭目的のサイバー犯罪などの標的になるといった、情報セキュリティ上の懸念が顕在化してきています。

（出典：「情報家電におけるセキュリティ対策　検討報告書」独立行政法人　情報処理推進機構）

Q17/22 インターネットに接続してゲーム機器や、デジタルテレビなどの情報家電を利用するときに、情報セキュリティ対策として意識しておくべき対応のうち、間違っている選択肢はどれでしょうか？

【解答】

A3. 機器の取扱説明書に記載された設定を行ったので、それ以上特に利用時に意識しておくことはない

【解説】

ゲーム機器やデジタルテレビなどの情報家電に搭載されているＯＳやソフトウェアにも、セキュリティホールが発見される場合があり、これらの情報家電においても、パソコンなどと同様に修正プログラム（セキュリティパッチ）がメーカーから無料で提供されています。インターネットに接続される機器は、ウイルス感染やスパイウェア、ボットなどの攻撃対象となりえるため、提供された修正プログラムはすぐに適用して、セキュリティホールの修正を行いましょう。よってＡ１は正しい対応です。

したがってA3のように、機器の取扱説明書に記載された設定を行っただけで、セキュリティ対策は完ぺきということにはなりません。よってA３は適切な対応ではありません。

また、漏えいしたら困る情報については、情報家電において扱う場合でも、パソコンからの利用時と同様の注意が必要です。よってＡ２は正しい対応です。

【参考】

あるゲーム機器では、セキュリティホールが発見され、修正プログラムが公開されました。

今後、情報家電などの多機能化に伴い、パソコンなどと同じように、修正プログラム情報の公開が増えてくることが予想されます。

１１． SNSやブログ利用時の注意事項

Q18/22 **SNSやブログの利用に関して、情報セキュリティの観点から間違っている選択肢はどれでしょうか？**

【解答】
A1. SNSやブログで知り合った人との交流を広げるためにも、自分のプライバシー情報は積極的に公開して、相手から信頼を受けるようにしている

【解説】
SNSやブログでは、参加者が本人であるか確認しにくいため、なりすましの可能性が疑われる場合には、本人から直接得ている連絡先等に事実確認をするとよいでしょう。よってＡ2は正しい選択肢です。
また、コミュニケーションを楽しむコミュニティであるからこそ、様々な人が参加しているので、日記に掲載する写真は、公開しても誰も困らないようなものを選択するなどの配慮も必要です。よってＡ３は正しい選択肢です。
コミュニケーションを楽しみたいがために、自分のプライバシーを積極的に公開することは、正しい行動とはいえません。よってＡ１は間違った選択肢です。

Q19/22 **スマートフォンを通じてSNSやブログに情報を公開することに関して間違っている選択肢はどれでしょうか？**

【解答】
A3. 街中でスマートフォンで撮影した写真に他人が写っている場合、自分とは関係のない人なので、特に配慮することなく公開しても問題はない

【解説】
スマートフォンで撮影した写真には、位置情報が記録されている場合があります。このことを知らずに、自分で撮影した写真データをブログなどに公開した場合、それを閲覧した人から、撮影位置を特定されることになります。自宅の写真を公開した場合には、自宅が特定されることになります。このため、居場所の情報が知られたくない場合は、写真データのプロパティに記録されている位置情報を加工するなどして、公開しても位置情報を知られないよう取り扱いましょう。よってＡ１は正しい選択肢です。
また、SNSやブログのプロフィール（氏名や顔写真などの個人を特定する情報、電話番号など）で公開する情報は、誰の目に触れるかわかりません。ストーカーなどの被害も考えられるため、適切に取捨選択したうえでの利用が求められます。よってＡ２は正しい選択肢です。
一方、Ａ３については、Ｑ１０の解説と同様に、写真に写ってしまった人のプライバシーを侵害する可能性があるので、顔を特定できないよう加工するなど、配慮が必要です。よってＡ３が間違った選択肢です。

１２．自宅外利用時

Q20/22 紛失したら困る重要な情報が保存されたパソコンやスマートフォン、USBメモリなどを持って外出するときは、情報セキュリティ対策上、注意すべきこととして間違っている選択肢はどれでしょうか？

【解答】
A3. 重要な情報を持っていることを周囲に気づかれないよう、持っていることを忘れて、平常通りの行動をする

【解説】
紛失したら困る重要な情報の入ったパソコンやスマートフォンを持って外出するときは、紛失や盗難に気をつけましょう。USBメモリなどの小さなものの紛失にも気をつけましょう。よってＡ１は正しい選択肢です。
また、気を付けていても紛失する場合が考えられます。そこで、予め紛失したときのことを想定して、パソコンやスマートフォンなどには起動時にパスワードを入力するよう設定しましょう。USBメモリの場合は、中のファイルにパスワードを設定しておきましょう。よってＡ２は正しい選択肢です。

Ａ３のように、注意力を持たない行動は紛失に繋がりかねないので、正しい選択とは言えません。情報漏えいなどのセキュリティ事故は、人の注意不足によるものが多いことからも、セキュリティに対する意識を保つことの重要性が指摘されています。よって、Ａ３は間違った選択肢です。

Q21/22 外出先で無線LANに接続してインターネットを利用する場合のセキュリティに関する注意として間違っている選択肢はどれでしょうか？

【解答】
A2. 電波を利用した通信形態をとる無線LANは盗聴される心配はない

【解説】
無線LANは、電波を利用して通信を行うため、電波の届く範囲であれば、どこからでもネットワークに接続ができる便利な仕組みです。一方で、発信された電波は第三者でも傍受することが可能であるため、盗聴される危険性があります。よってA2は間違った選択肢です。

無線LANには、盗聴を防ぐために暗号化の機能が用意されていますが、中には解読されやすい暗号化方式を採用しているアクセスポイントもあります。漏えいして困るような情報は安易に扱わないように注意することが大切です。よってＡ３は正しい選択肢です。

また、無線LANを通じて第三者から自分のパソコンを侵害されることを防ぐために、ファイアーウォール機能を有効にしておくことも適切な対策です。よってＡ1は正しい選択肢です。

13．トラブル発生時の対応

Q22/22 **インターネット利用時にコンピュータのセキュリティに何か異常を感じたとき(例えば、架空請求のメールが届いたり、開いているページを閉じることができないなど)の対応として間違っている選択肢はどれでしょうか？**

【解答】

A1. 数か月様子を見て、それでも異常を感じるようだったら、誰かに相談する

【解説】

インターネット利用時に、不審なファイルを実行してしまって以来パソコンの動作がおかしい、開いているページを閉じることができないなどの異常を感じたら、コンピュータがウイルスに感染している可能性があります。ウイルス感染は、自分1人のトラブルだと考えがちですが、実は周りにも迷惑をかけてしまうことがあります。例えば、他の人のパソコンに自分のパソコンが攻撃を仕掛けることもあります。

このようなトラブルが発生したときには急いで対応することが必要です。時間がたってからでは、ウイルス感染による被害が拡大します。よってA1は間違った対応です。

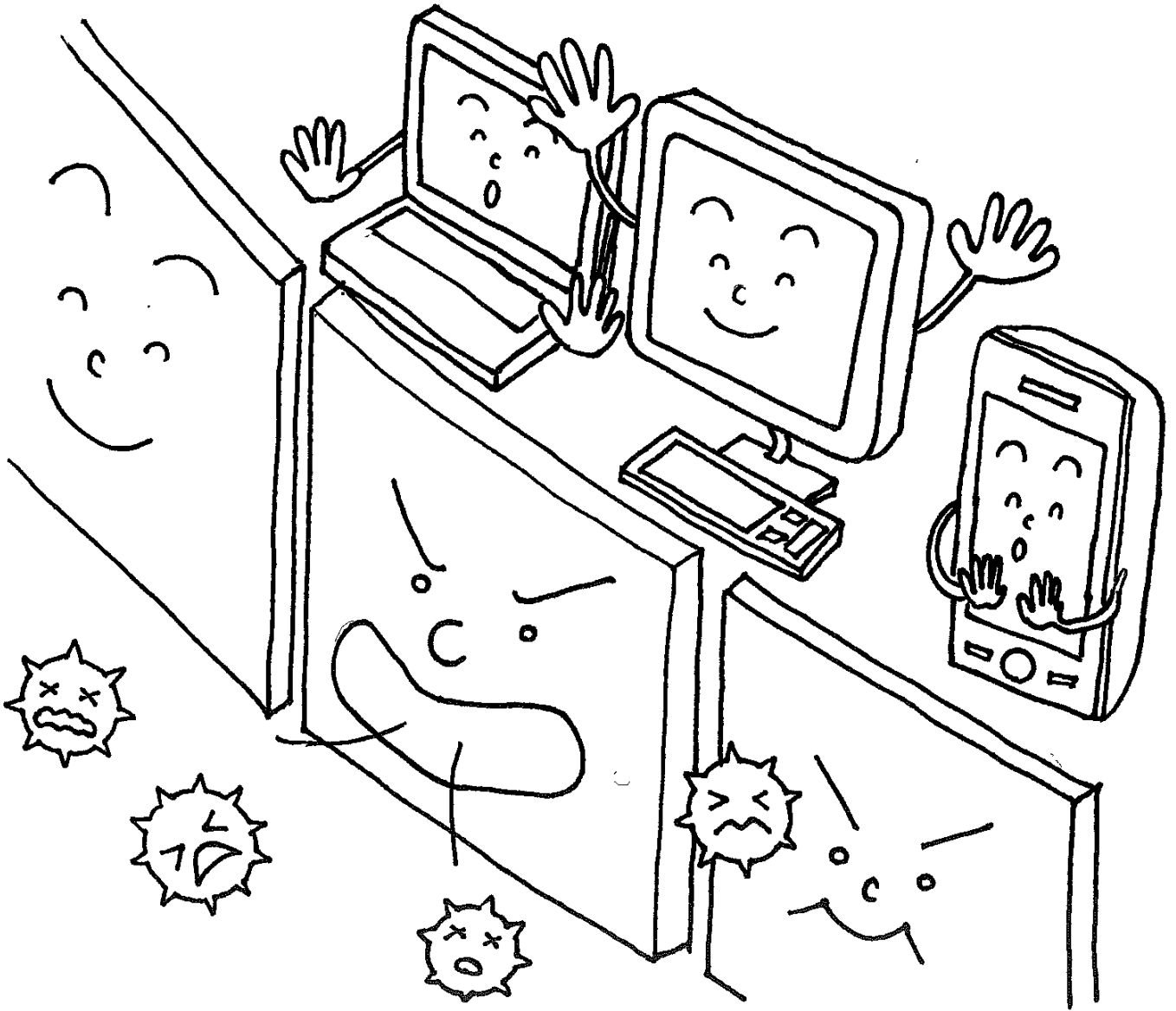
ウイルス感染時の行動は、まずウイルスに感染したと思われるパソコンをネットワークから切り離すことで感染が広がらないようにします。よってA２は正しい対応です。

また、ウイルス感染だけでなく、架空請求やワンクリック詐欺などのトラブルに遭ったら、1人で悩まず誰かに相談しましょう。近所のセキュリティに詳しい人や、以下の情報セキュリティ相談窓口に症状に応じて相談するとよりスムーズにトラブルを解決できるかもしれません。よってA3は正しい対応です

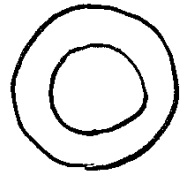
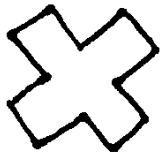
- 購入した製品の具体的な使い方については取扱説明書などに記載されている連絡先へご連絡ください
  - ✓各製品の開発元/販売元
  - ✓電話番号　各製品の取扱説明書などに記載されています
- コンピュータウイルスに感染してしまったと思ったらこちらにご相談ください
  - ✓IPA(情報処理推進機構)セキュリティセンター　安心相談窓口
  - ✓電話番号　03-5978-7509(平日10:00～12:00 および 13:30～17:00)
- 広告や宣伝目的の迷惑メールに困っている時はこちらへご連絡ください
  - ✓財団法人日本データ通信協会　迷惑メール相談センター
  - ✓電話番号　03-5974-0068(平日10：00～17：00)(祝祭日は除く)
- 犯罪に係る相談や情報提供を電話で受け付けています
  - ✓各都道府県警察のサイバー犯罪相談窓口
  - ✓電話番号　各都道府県警察にお問い合わせ下さい

別添資料3

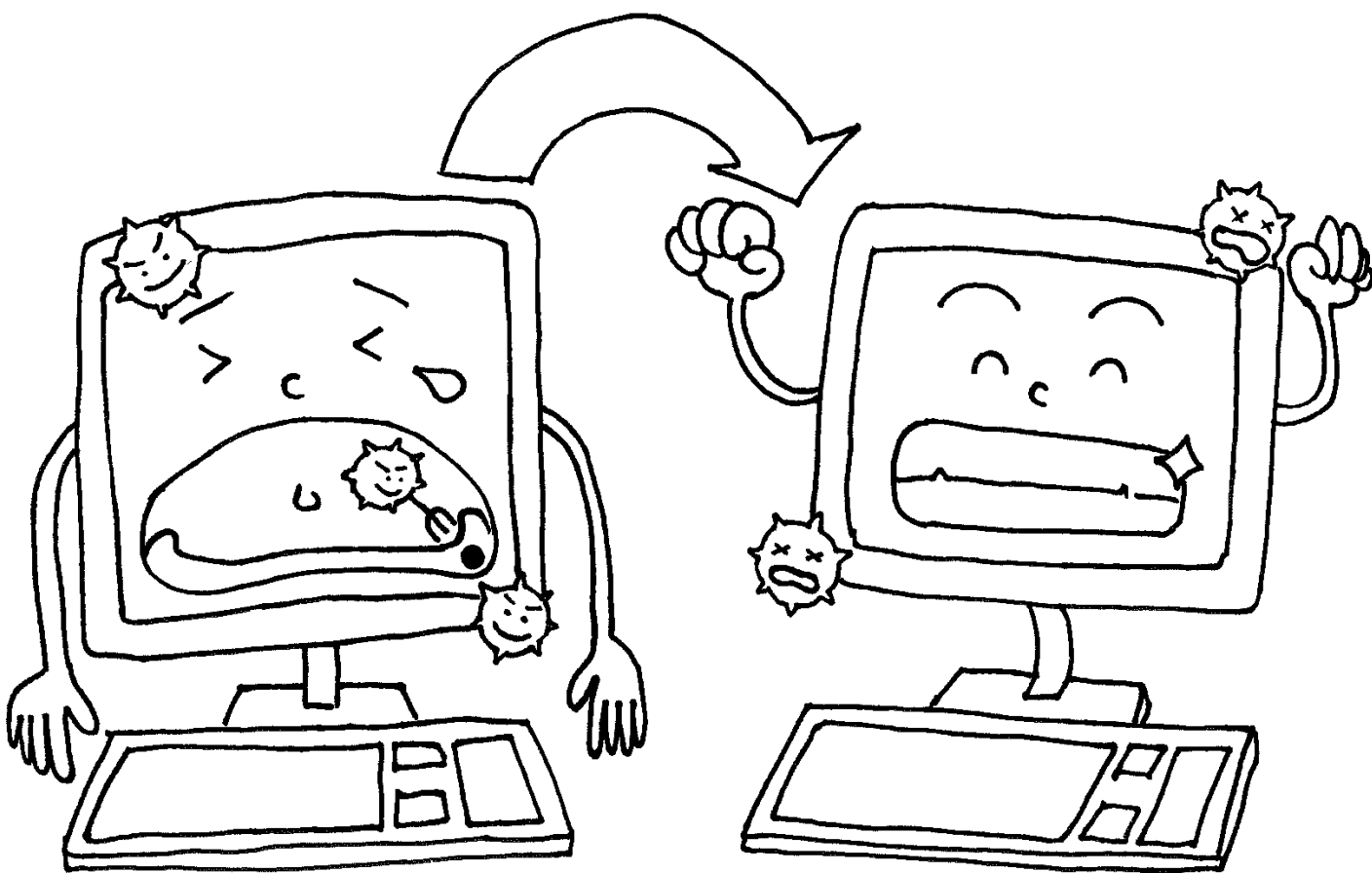
高齢者向け資料（ポスター）

ウイルス対策ソフトを導入しよう！

　わたしたちの世界で風邪のウイルスが存在するように、コンピュータの世界にも、コンピュータに悪さをするウイルスが存在します。

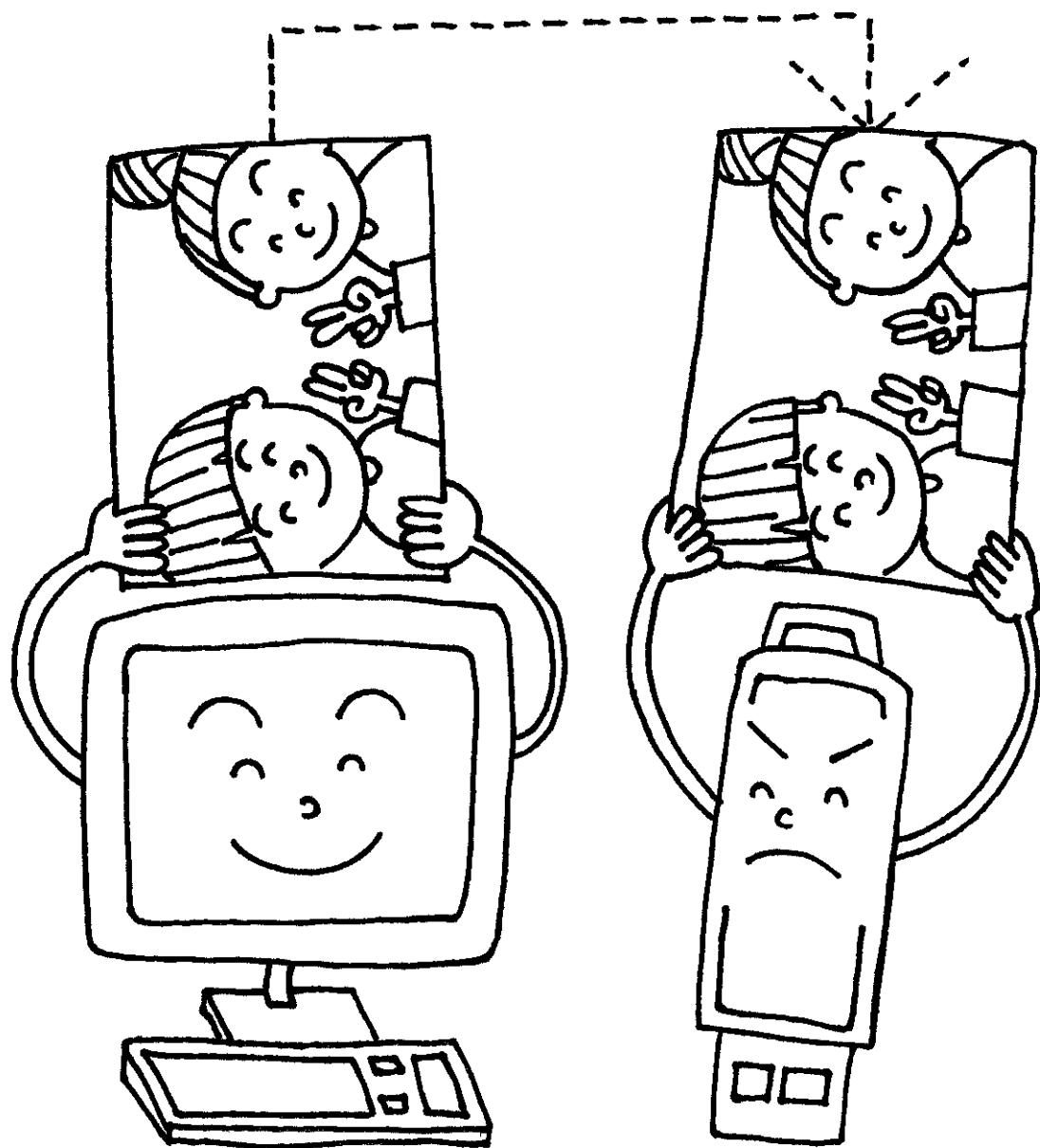
　コンピュータウイルスに感染しないように、家電量販店などでウイルス対策ソフトを入手し、コンピュータに導入しましょう！

パスワードは貴重品のように管理しよう！

パソコンやスマートフォンの起動画面に、他人から容易に推測されないパスワードを設定しておくことは、自宅に鍵をかけるのと同じように大切なことです。

パスワードは他人に知られないようにする必要があります。
メモに残さざるを得ない場合、人の目に触れない場所に保管しましょう。

OS（オーエス）やソフトウェアは常に最新の状態にしておこう！

パソコンやスマートフォンは、新たに発生するコンピュータウイルスの攻撃に対抗できるよう、頻繁に製造元が改良を加えています。

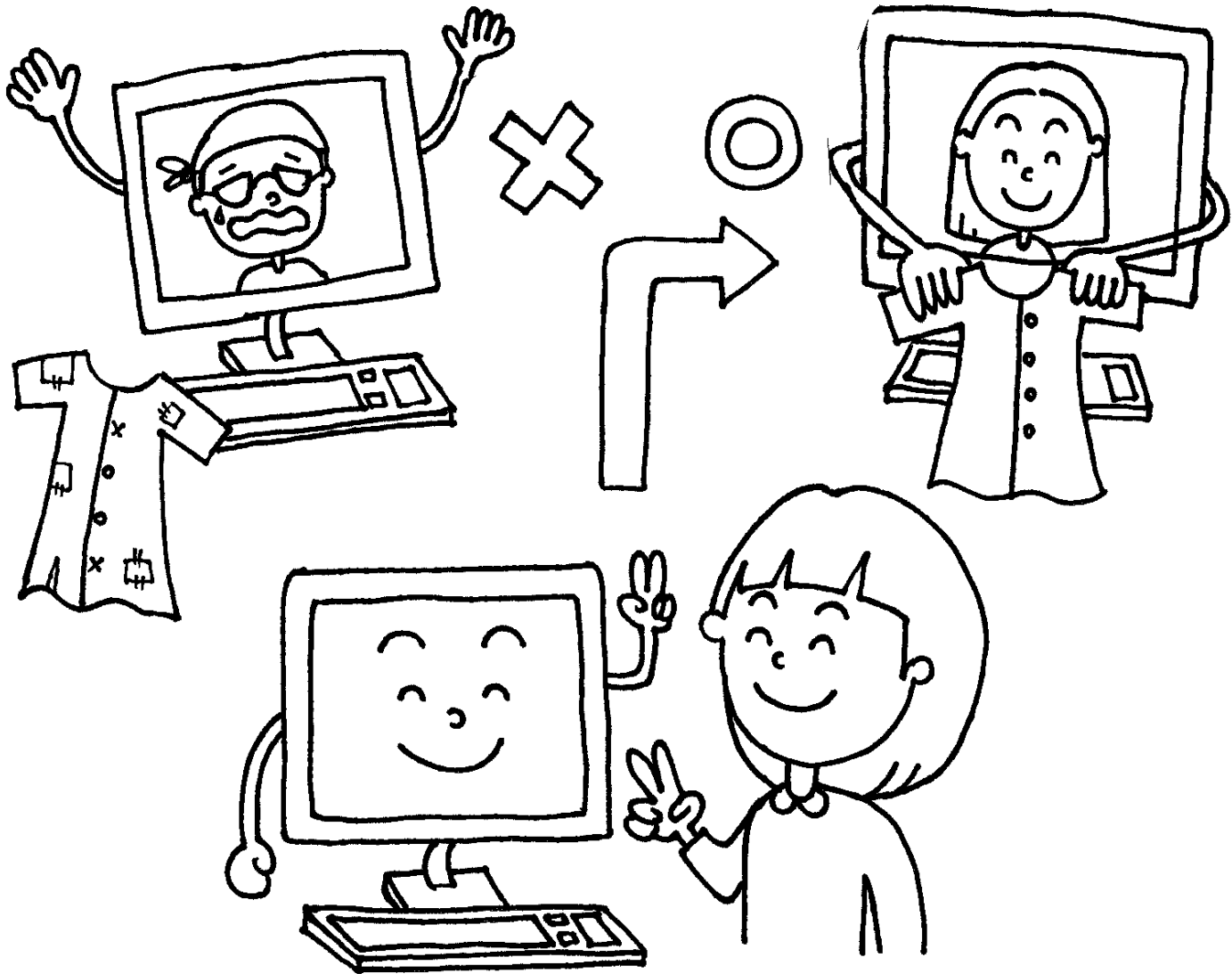
製造元から無料で配布される最新の改良プログラムを入手して、コンピュータウイルスの攻撃に対抗できる強い環境を手に入れましょう！！

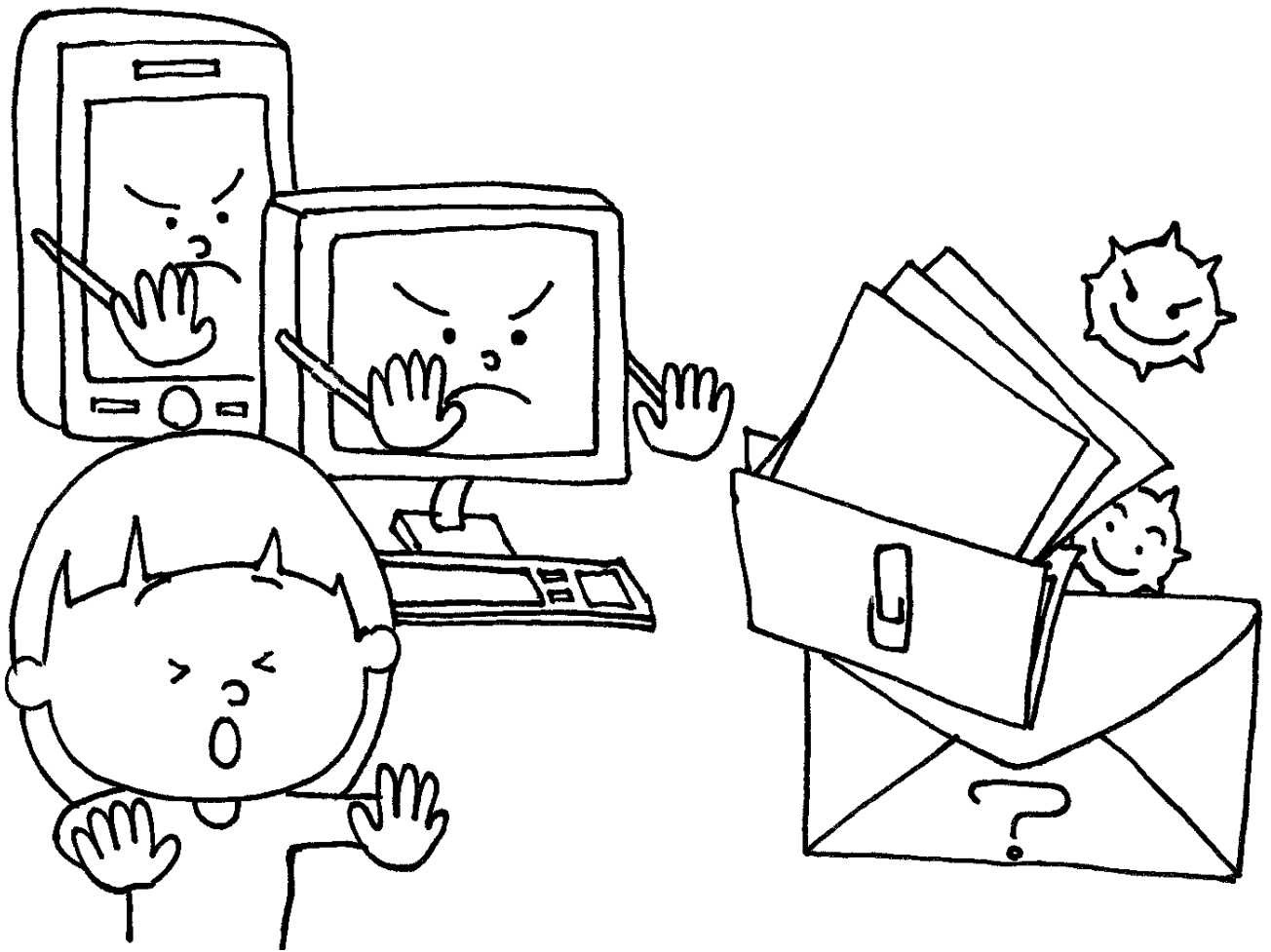
大切な情報は
失う前に複製しよう！

家族や友人と一緒に撮影した思い出の写真のように、失ったら困る情報には、USB(ユーエスビー)メモリなどに複製（バックアップ）して、保管しておきましょう！！

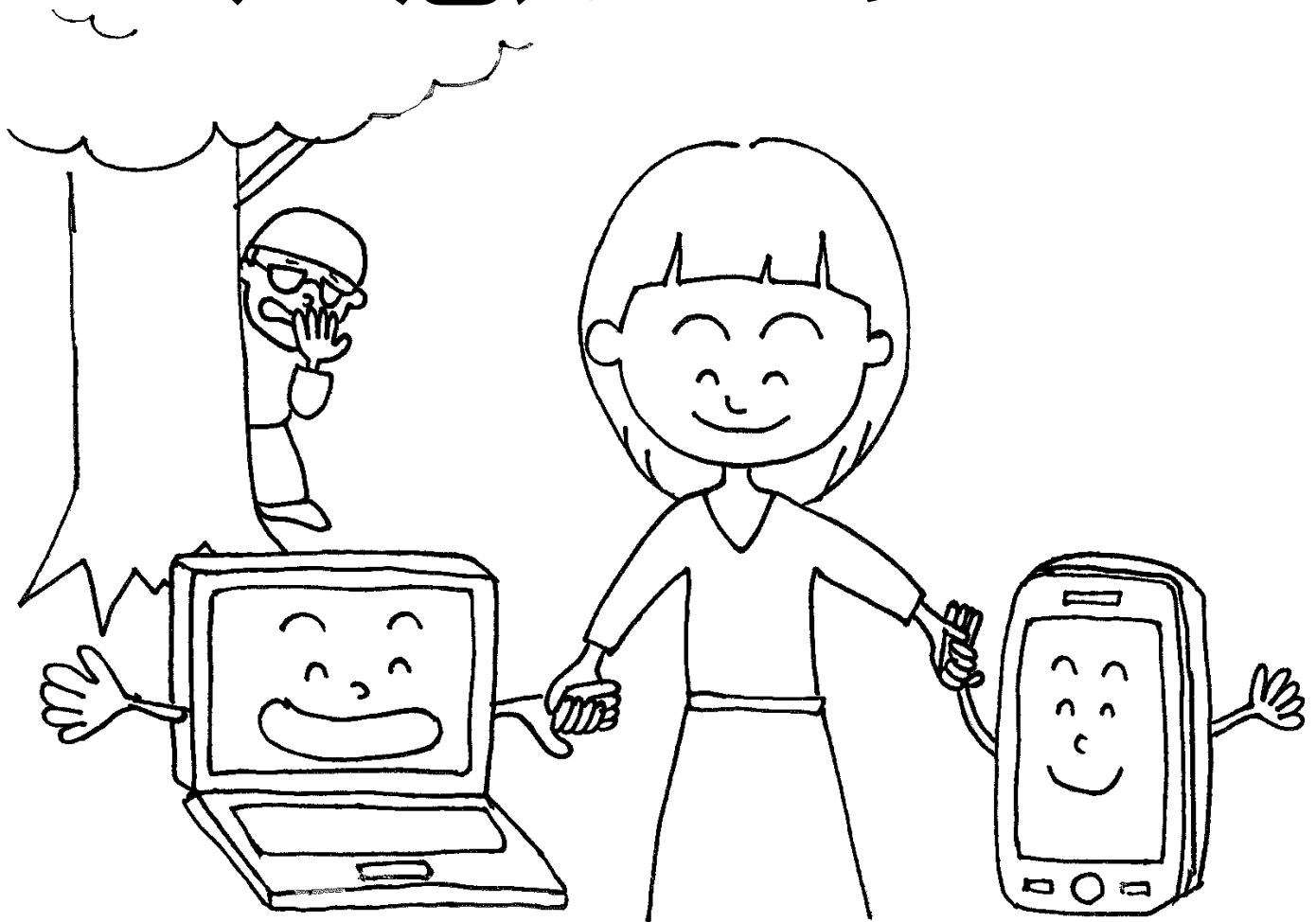
ログインID（アイディー）・パスワード 絶対教えない 用心深さ

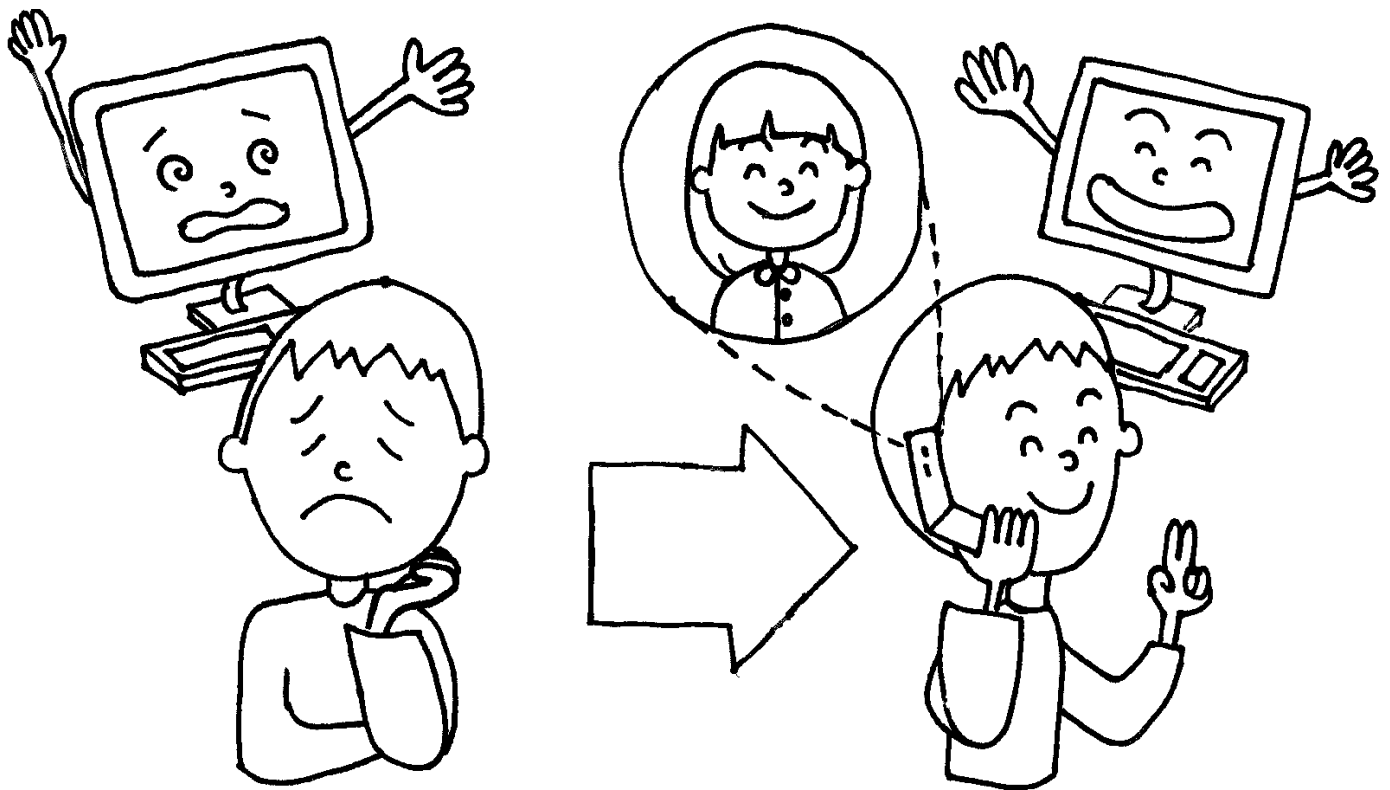
金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すようなメールが届いた場合、教える必要はありません。

身に覚えの無いメールには返信せずに無視するなど、安易に教えないよう注意しましょう。

ネットショッピングでは信頼できるお店を選ぼう！

ネットショッピングでは、品物だけでなく、見たい映画や聴きたい音楽も購入することができます。ネットショッピングをするときは、詐欺などの被害に遭わないように信頼できるお店を選びましょう！身近な人からお勧めのお店を教わるのも安心です。

身に覚えのない添付ファイルは開かない！

身に覚えのない電子メールには、コンピュータウイルスが潜んでいる可能性があります。ウイルス感染を予防するために、身に覚えのない電子メールに添付されたファイルは開かないようにしましょう！！

外出先では紛失・盗難に注意しよう！

大切な情報を保存しているパソコン、スマートフォンやUSB（ユーエスビー）メモリなどを自宅の外に持ち出すときは、持ちだす機器やファイルにパスワードを設定し、貴重品を扱うのと同様、なくしたり盗まれないよう注意して持ち歩きましょう！！

困った時は
ひとりで悩まず
まず相談！

　インターネット利用に関する被害相談として、架空請求の電子メールが大量に届いたり、開いているウェブページをどうしても閉じることができないというような相談が増えています。

　このような症状が見られたら、ひとりで悩まず、身近な人に相談すると良いでしょう。

別添資料3

高齢者向け資料（リーフレット）

★ 各種相談窓口

●購入した製品の具体的な使い方については取扱説明書などに記載されている連絡先へご連絡ください
　✓各製品の開発元/販売元
　✓電話番号　各製品の取扱説明書などに記載されています

●コンピュータウイルスに感染してしまったと思ったらこちらにご相談ください
　✓IPA（アイピーエー）(情報処理推進機構)セキュリティセンター　安心相談窓口
　✓電話番号　03-5978-7509(平日10:00～12:00 および 13:30～17:00)

●広告や宣伝目的の迷惑メールに困っている時はこちらへご連絡ください
　✓財団法人日本データ通信協会　迷惑メール相談センター
　✓電話番号　03-5974-0068(平日10：00～17：00)(祝祭日は除く)

●犯罪に係る相談や情報提供を電話で受け付けています
　✓各都道府県警察のサイバー犯罪相談窓口
　✓電話番号　各都道府県警察にお問い合わせください

★ (参考)パソコンなどの機器ごとに利用できる機能

機器		パソコン	デジタルテレビ	スマートフォン	ゲーム機器
利用できる機能	インターネット ネットショッピング 電子メール	○	○	○	○
	テレビ電話	○		○	
	ゲーム	○		○	○
	テレビ	○	○	○	

インターネットを安全に利用するための
情報セキュリティ対策9カ条

インターネットの利用は生活の幅を広げるだけでなく、
災害時には自分の命を支える手段にもなります。
情報セキュリティを正しく学ぶことで、
安全・快適にインタ-ネットを使いましょう。

★ インターネットの利用は、日常生活の幅や人との触れ合いを拡げることができます！

　インターネットの利用は、自宅に居ながらにしてネットショッピングができたり、人とコミュニケーションしたり、欲しい情報を収集することが可能です。

★ 災害時には自分の命を支えてくれます！

　先の震災時には、携帯電話やスマートフォンなどの携帯通信端末を所有していた人は、停電などによりテレビが使えなくても、インターネットなどを利用して情報を収集できました。このため、避難場所の情報や支援物資の配給場所などを把握したり、安否確認などのコミュニケーションツールとして有益であったため、災害には自分の命を支える手段になることが示されました。

　このハンドブックでは、安全にインターネットを利用して便利な生活を送るための、最低限やっておくべき９カ条をまとめています。

　９カ条を実践して、便利で快適なインターネットライフを充実させましょう！

インターネットを安全に利用するための
情報セキュリティ対策　9カ条

1. 利用環境の設定
2. パスワードの設定
3. セキュリティの更新
4. 紛失したら困る重要情報の取り扱い
5. 金融財産情報の取り扱い
6. デジタルコンテンツの入手・視聴
7. 電子メール利用時
8. 自宅外利用時
9. トラブル発生時

1 ウイルス対策ソフトを導入しよう

わたしたちの世界に風邪のウイルスが存在するように、コンピュータの世界にもコンピュータに悪さをするウイルスが存在します。

ウイルスに感染しないように、コンピュータにウイルス対策ソフトを導入しましょう。（ウイルス対策ソフトは家電量販店などで入手できます）

2 パスワードは貴重品のように管理しよう

パソコンやスマートフォンの起動画面にパスワードを設定しておくことは、自宅に鍵をかけるのと同じように大切なことです。

パスワードは他人に知られないようにする必要があります。メモに残さざるを得ない場合、人の目に触れない場所に保管しましょう。

3 OSやソフトウェアは常に最新の状態にしておこう

パソコンやスマートフォンは、新たに発生するコンピュータウイルスの攻撃に対抗できるよう、頻繁に製造元が改良を加えています。

製造元から無料で配布される最新の改良プログラムを入手して、コンピュータウイルスの攻撃に対抗できる強い環境を手に入れましょう。

4 大切な情報は失う前に複製しよう

家族や友人と一緒に撮影した写真など、思い出がつまった情報は、パソコンの故障などにより失われてしまうと、取り返しがつきません。

大切な情報は、USBメモリなどに複製して、保管しておきましょう。

5 ログインID・パスワード絶対教えない用心深さ

金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すようなメールが届いた場合、教える必要はありません。

身に覚えのないメールは返信せずに無視するなど、安易に教えないよう注意しましょう。

6 ネットショッピングでは信頼できるお店を選ぼう

ネットショッピングでは、品物だけでなく、見たい映画や聴きたい音楽も購入することができます。

ネットショッピングをするときは、詐欺などの被害に遭わないように、信頼できるお店から買うようにしましょう。身近な人からお勧めのお店を教わるのも安心です。

7 身に覚えのない添付ファイルは　開かない

身に覚えのない電子メールには、コンピュータウイルスが潜んでいる可能性があります。

ウイルス感染を防ぐために、身に覚えのない電子メールに添付されたファイルは開かないようにしましょう。

8 外出先では　紛失・盗難に注意しよう

大切な情報を保存しているパソコン、スマートフォンや、USBメモリなどを自宅の外に持ち出すときは、機器やファイルにパスワードを設定し、貴重品を扱うのと同様、なくしたり盗まれないように注意して持ち歩きましょう。

9 困ったときは ひとりで悩まず　まず相談

インターネット利用に関する被害相談として、詐欺や架空請求の電子メールが届く、開いているウェブページをどうしても閉じることができないというような相談が増えています。

このような症状が見られたら、一人で悩まず、症状に応じ相談窓口(背表紙参照)に相談しましょう。

別添資料 5

国内事例集

2012年3月

株式会社 NTT データ経営研究所

目次

1.　情報セキュリティ分野における自己診断チェックリスト　事例調査結果

1.1.　サマリー

情報セキュリティ分野における自己診断チェックリストに係る国内の取組事例を取りまとめた。

※1　インターネットを介さない配布媒体
※2　インターネットを介した配布媒体
※3　日本ネットワークセキュリティ協会
※4　情報処理推進機構

事例	取組機関	分野	対象	様式		配布媒体		
				段階評価型	クイズ形式	アナログメディア※1	デジタルメディア※2	イベントサポータ支援
情報セキュリティ認識度チェック	総務省	情報セキュリティ	国民 企業		○		○	
セキュリティクイズ	経済産業省	情報セキュリティ	国民		○		○	
理解度セルフチェック	JNSA※3	情報セキュリティ	企業		○		○	
セキュリティ対策チェックシート	IPA※4	情報セキュリティ	企業	○			○	

図 1　情報セキュリティ分野における自己診断チェックリスト　事例調査結果サマリー

1.2.　情報セキュリティ認識度チェック　(総務省)

①作成指針

情報セキュリティ認識度チェックリストを含め、同チェックリストが掲載されている情報セキュリティサイトは、これから情報セキュリティ対策を講じようとする国民の一助となることを目的としている。

チェックリストは、3種（小学生用、一般国民用、企業組織用）が存在し、それぞれが日常で遭遇する可能性があるケースに基づいてチェック項目を作成している

②目的対象

小学生、一般国民、企業組織の 3 つの分野を対象としており、各情報セキュリティについて、どのくらい理解しているかを確認するツールとして利用してもらうことを目的としている。

③配布方法

総務省のホームページ上(http://www.soumu.go.jp/main_sosiki/joho_tsusin/joho_tsusin.html)にウェブアプリケーションとして組み込まれている。紙媒体での配布は実施されていない。

図 2　情報セキュリティ認識度チェックリスト　サイトイメージ[1]

[1] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/security_check/s_check.htm

④チェックリストの様式

問題は小学生、一般国民、企業組織用、いずれも三択クイズ形式となっており、5～7問で構成されている。全て解答するまでの所要時間は5分程度である。質問項目の内容は、ケーススタディ形式となっており、それぞれの対象において具体的な利用場面がイメージできるようなチェック項目の内容となっている。そのため、小学生、一般国民、企業組織用でチェック項目の内容は異なっている。

各チェック項目に解答する毎に、解説が表示され、どの選択肢が何故正解なのか、またその場面ごとにやるべきことや注意すべきことなどを紹介している。

以下に実際に一般国民用の自己診断チェックリストで出題されているチェック項目を例として示す。

■情報セキュリティ対策に関する問題

Q1 どのような場面においても情報セキュリティ対策は大切なものです。次の中で正しいものはどれでしょうか？

A ウイルス対策ソフトの使用期限が切れた。ウイルス対策ソフトが動いていても、直ちに継続するためのライセンスを購入するか、新たに購入するかしなくてはならない。

B 引っ越したばかりで、パーソナルファイヤーウォールもブロードバンドルータも持っていない。いずれかを購入するために短時間インターネットをつないだ。

C OSやソフトウェアへのパッチの適用は、手間がかかるので、毎年、年末にまとめて行っている。

■パスワードに関する問題

Q2 適切なパスワードは情報セキュリティ対策の基本となります。パスワードについて、次の中で誤りでないものはどれでしょうか？

A 忘れてしまうと困るので、自分が応援しているサッカーチームの名前をパスワードにしている。

B 忘れてしまうと困るので、パスワードを紙に書いて鍵のかかる自分の引き出しにしまっている。

C 忘れてしまうと困るので、自分が使うパスワードは昔から統一して同じものを使い続けている。

■迷惑メール対策に関する問題

Q3 受け取りたくない迷惑な電子メール（迷惑メール）を減らすための対応として、次の中で誤っているものはどれでしょうか？

A 長くて分かりにくいメールアドレスを使う。

B あらかじめ決めておいたメールアドレスやドメインから電子メールしか受け取らないようにしておく。

C 電子メールを送ってきた人に返事を書いて、もう送ってこないように伝える。

■ファイル共有ソフトに関する問題

Q4 ファイル共有ソフトを使う上での危険性の認識として、正しいものはどれでしょうか？

A ファイル共有ソフトは、目的のファイルをダウンロードすると同時に自分のPCのファイルを公開するため、ウイルスなどに感染すると、公開して欲しくないファイルも公開されてしまう

B ファイル共有ソフトではウイルスが多く流通しているが、ファイル名やアイコンを確認することでウイルスかどうかは簡単に判別できる。

C ファイル共有ソフトで一旦流出してしまったファイルは取り消すことは簡単だが、流出したことに気づきにくいのが問題だ

図3　一般国民用の自己診断チェックリスト　出題チェック項目例[2]

[2] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/security_check/s_check.htm (様式のみ NTT データ経営研究所が修正)

1.3.　セキュリティクイズ　(経済産業省)

①作成指針

　誰でも容易にインターネットに接続できるようになった今日、コンピュータウイルスの感染、不正アクセス、フィッシング詐欺等の被害に遭遇する危険性が高まっており、このような被害を未然に防ぎ、安心して IT を利用するための意識及び知識の向上を図るためにセキュリティクイズをはじめとした情報セキュリティの普及啓発活動を実施している。

②目的対象

　一般のインターネット利用者を対象に、コンピュータウイルスの感染や不正アクセス、フィッシング詐欺などの被害を未然に防ぐことを目的としている。

③配布方法

　経済産業省のホームページ上(http://www.meti.go.jp/press/20070122003/20070122003.html)にウェブアプリケーションとして組み込まれている。紙媒体での配布は実施されていない。

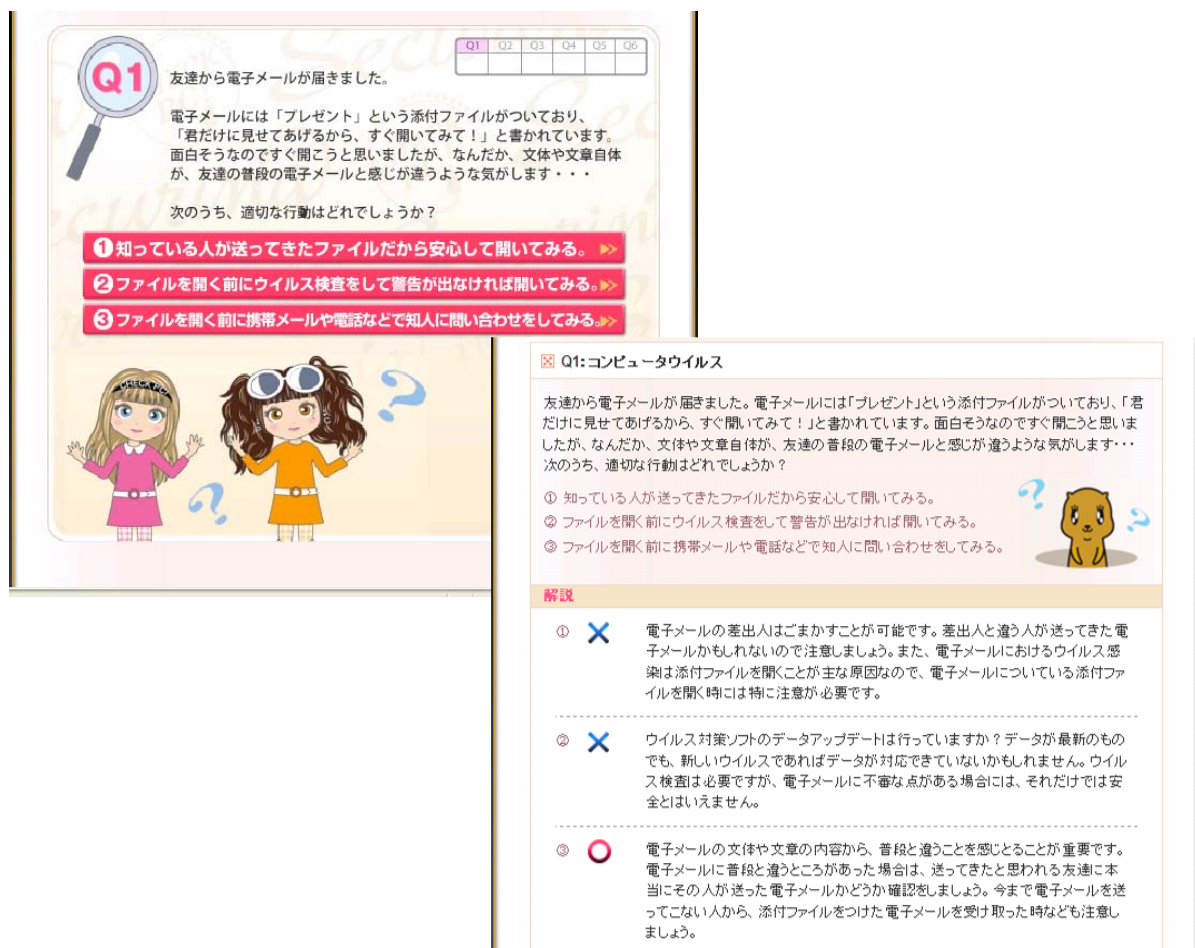



図 4　セキュリティクイズ　サイトイメージ[3]

[3] http://www.checkpc.go.jp/quiz/detail.html#contents_head

④チェックリストの様式

問題は、3 択クイズ形式で問題数は全 6 問であり、所要時間は 5 分程度である。総務省が紹介する「情報セキュリティ認識度チェックリスト」のように小学生、一般国民用、企業組織用などの分類はなく、広く一般国民を対象としている。

チェック項目の内容は、一般国民が日常生活の中でインターネットなどの IT サービスを利用する場面ごとにチェック項目を作成している。例えば、電子メールをテーマとした問題では、友人からメールが届き「添付ファイルを開いてみて」と本文には書かれているのだが、文体が普段の友人から届く電子メールとは違う感じがするなどのように、なりすましメールの 1 場面を具体的に記載し、一般国民でも具体的な場面をイメージできるように工夫がされている。

全てのチェック項目解答後には、各選択肢に対して何故正解か、何故不正解かをその理由を 1 問毎に解説をしており、正しいことと間違っていることの分別を付けることができるように工夫されている。

以下に実際に出題されているチェック項目例を示す。

Q2
友達から「君の好きな商品がたくさんある激安おすすめショッピングサイトを教えてあげるよ！！」とサイトを紹介されました。サイト利用には、ID・パスワードを登録（ユーザ登録）しなければなりません。早速、ユーザ登録を行おうと思います・・・・・

IDパスワードを考えるにあたって、適切な行動はどれでしょうか？

①覚えやすいように自分の名前をID、誕生日をパスワードにする

②他のサイトデモ使っているID・パスワードと同じものを使う

③このショッピングサイトだけで使うID・パスワードを考える

Q3
インターネットには様々な情報が溢れていますが、その中には、著作権侵害となる画像や動画、わいせつ情報、違法薬物販売情報、犯罪をそそのかす情報等の違法・有害情報が存在します。あちらこちらのウェブサイトを見ている間に、これらの情報を見にしてしまう危険性があります。子供たちを違法・有害情報から守る対策として適切なものはどれでしょうか？

①有害情報、違法情報を公開しているようなウェブサイトへのアクセスを防止するフィルタリングソフトウェア、フィルタリングサービスを利用する。

②ウェブページのタイトルやURLリンクのドメイン名簿に注意し、怪しいサイトに近寄らないようにする。

③ウイルス対策ソフトウェアをインストールし、ウイルス定義ファイルの更新を行う。

図 5　セキュリティクイズ　出題チェック項目例[4]

[4] http://www.checkpc.go.jp/quiz/detail.html#contents_head (様式のみ NTT データ経営研究所が修正)

1.4.　理解度セルフチェック　(JNSA ：日本ネットワークセキュリティ協会)

①作成指針

　パソコン利用者が自分の情報セキュリティの理解度レベルを客観的に把握し、適切な情報セキュリティ知識を身につけ、セキュリティ上の問題に正しく対応できるようなチェック項目を作成している。

②目的対象

企業で働く人々を対象としており、利用者一人一人が情報セキュリティについて理解を深めるために、情報セキュリティの理解度を各人に確認してもらうことを目的としている。

③配布方法

　JNSAのホームページ上(http://www.jnsa.org/)にウェブアプリケーションとして組み込まれている。紙媒体での配布は実施されていない。

図 6　理解度セルフチェック　サイトイメージ[5]

---

[5] http://slb.jnsa.org/slbm/

④チェックリストの様式

チェックリスト項目は全て 4 択クイズ形式で計 25 問である。所要時間は 30 分程度である。チェック項目の内容は、チェック項目の内容が理解しやすいように、企業内でパソコンやインターネット接続機器を利用する場面毎にその時々の正しい行動や考え方を問う様式と、情報セキュリティに関する知識を問う様式の 2 つが混在した内容となっている。後者の例としては、「セキュリティ区画の考え方で最も不適切なものはどれでしょうか？」などが挙げられる。

チェック項目は以下の 8 つの分野で構成されている。

1. 電子メールの知識と利用法
2. ウイルスの知識と対処方法
3. インターネットの利用法と注意点
4. パスワードの知識と管理
5. PC の利用上の注意点
6. オフィスにおける情報セキュリティ
7. ルールや規則の遵守
8. 社外における情報セキュリティ

以下にチェック項目の例を数問示す。

Q1
ホームページを閲覧していたら、「ウイルスに感染しました。」とポップアップが表示され、さらに、「ウイルスを削除するために指定されたURLのウイルス対策ソフトをインストールしてください。」と表示されました。このときの対応として適切でないものはどれでしょうか？

1. メッセージ通り指定されたウイルス対策ソフトをインストールし、ウイルススキャンする
2. 無視する
3. どうすればよいかわからないため、システム管理者に問い合わせる
4. 既存のウイルス対策ソフトでウイルススキャンする

Q2
USBメモリ等によるデータの持ち出しで適切でない行動は、次のうちどれでしょう？

1. 個人情報が入っていなければ、USBメモリに入れて、持ち出してもかまわない
2. データは、暗号化してから、USBメモリに入れる
3. データを持ち出す場合は、組織で決められた手続きを済ませてからおこなう
4. パスワードを設定してから、USBメモリに入れる

Q3
パソコンで作業中に上司に呼ばれて離席します。パソコンの適切な処理はどれでしょうか？

1. OSのコンピュータロックをかけるか、パスワードつきスクリーンセーバーを起動する
2. 直ちにアプリケーションを終了する
3. スクリーンとキーボードに紙をかぶせる
4. 席に戻った時すぐに仕事を続けられるように、作業中のウインドウをそのままにしておく

図 7　理解度セルフチェック　出題チェック項目例　(1/2)[6]

[6] http://slb.jnsa.org/slbm/　(様式のみ NTT データ経営研究所が修正)

Q4
セキュリティ区画の考え方で最も不適切なものはどれでしょうか？

1. ビルへ入る際IDカードが必要なので、セキュリティ区画となっている部屋へのアクセス制御は不要
2. セキュリティ区画が業務区画と同じフロアにあるが、権限のないものは入室できないように施錠されている
3. セキュリティ区画への入室権限が無くても、管理者の許可があれば入室は可能である
4. セキュリティ区画は、その情報管理の重要度レベルによって、複数設定される事もある

Q5
携帯電話のメールアドレスに迷惑メールを受信しないようにするために気をつけることとして、最も適切でないものはどれでしょうか？

1. 見知らぬ人に安易に自分のメールアドレスを教えない
2. 短くて簡単なメールアドレスを使うようにする
3. 不用意に自分のメールアドレスをネット上に公開しない
4. ランダムにアルファベットや数字、記号を組み合わせたメールアドレスを使う

Q6
メールの盗聴を防ぐ手段として有効なものはどれでしょうか？

1. メールの暗号化
2. 加入しているサービスプロバイダのフィルタリングサービスの利用
3. Webメールの利用
4. 加入しているサービスプロバイダのウイルスチェックサービスの利用

図 8　理解度セルフチェック　出題チェック項目例　(2/2)[7]

⑤特記事項

計 25 問から構成されるクイズを全て解答すると、様式で紹介した 8 つの分野ごとに正答率のレーダーチャートが表示され、自分の得意、不得意分を確認することができる工夫がされている。

また、チェック項目の正解率と解答速度からランキングを付けてホームページ上にニックネームを公開するサービスも実施しており、利用者にチェックリストを単純に解答してもらうだけでなく、解答することへのインセンティブも同時に与える工夫をしている。

[7] http://slb.jnsa.org/slbm/　(様式のみ NTT データ経営研究所が修正)

1.5. セキュリティ対策チェックシート (IPA：独立行政法人情報処理推進機構)

①作成指針

IPA で独自に作成している「セキュリティ対策チェックシート作成の考え方」を指針としている。「セキュリティ対策チェックシート作成の考え方」では、情報システムのセキュリティを確保するためには、必要となる最新の情報の収集から始まり、不正アクセスを許す要因を極力減少させること、不正アクセス発生時にそれを発見し、然るべき対応・対策を取れることを念頭におき、チェックリストに反映させている

(1) 情報の収集をきちんと行っているか

セキュリティ情報の収集に努めるとともに、当該情報に基づく対策を講じることが必要か否か検討しているか。

（例：回覧板に「空き巣急増」といった記事があることをチェックしているか。それに基づき、家を少し空ける場合でも施錠するといった対策を行うか否か検討しているか。）

(2)不正アクセスにつながる要因を減らすための対策を行っているか

ネットワーク及びコンピュータに対する不正アクセスがなされないように、適切な対策を講じているか。

（例：きちんとした塀や門を設けているか。門に鍵はかけているか。鍵は適切に保管されているか。）

(3)不正アクセス及びその予備行為が行われたことを発見するための対策を行っているか

ネットワーク及びコンピュータに対して不正アクセスが行われた際にシステムに残される可能性のある痕跡を、きちんと確認しているか。

（例：塀や門を乗り越えられていないかモニターカメラ等で監視しているか。閉めたはずの鍵が、いつの間にか開けられていないか。）

(4)不正アクセスが行われた際の被害を軽減させるための対策を行っているか

不正アクセスが行われた場合にあっても、情報の改ざん、損失等が最小限にとどめられるよう、必要な対策をとっているか。

（例：貴重品は金庫に入れているか。通帳と印鑑は別々に保管しているか。）

(5)不正アクセスが行われた際に講じるべき対応を定めているか

不正アクセスが行われた場合に、状況を把握するためのログの保管や、対応方法、責任体制等を明確にしているか。

（例：現場保存。警察への通報。場合によっては、金融機関その他への届出等も必要。）

※不正アクセス技術は常に進歩しているため、最新の情報を収集することを怠らず、継続的に対策を更新、メンテナンスすることが重要である。

↓

情報が更新される毎に、チェックシートで確認する事項も更新する必要がある

図 9 セキュリティ対策チェックシート作成の考え方 IPA作成[8]

[8] http://www.ipa.go.jp/security/ciadr/checksheetappendix.html (様式のみ NTT データ経営研究所が修正)

②目的対象
企業で働く人々を対象に、情報システムに対するインターネットを経由した外部からの不正アクセスを予防するとともに、問題が生じた際の被害を軽減させることを目的としている。脅威の中でも、外部からの不正アクセスに対する対策のみを対象としている。

③配布方法
IPAのホームページ上(http://www.ipa.go.jp/security/ciadr/checksheet.html)に直接記載されている。紙媒体での配布は実施されていない。

④チェックリストの様式
チェック項目は全46問であり、全てYes/No形式である。チェック項目の内容は企業向けということもあり、日常生活へと応用できる情報セキュリティ対策の記載は少なく、多くのチェック項目が企業内で考えられる利用場面毎の行動や対応を問う形式で、専門性の高い内容となっている。チェック項目に対策実施の必要性に応じてA、B、Cの3つのレベルが付されており、チェックリスト利用者がどのチェック項目からまず取り組むべきか判断できるように工夫している。

Aランク：必ず対策を行うべきもの
Bランク：守るべき情報の重要性との兼ね合いではあるが、極力実施すべきもの
Cランク：守るべき情報の重要性と、当該項目の実施に必要なコストなどを勘定の上、必要と思われる場合には行うべきもの

1. 不正アクセスの要因を減少させるための対策

- **A(1)** 外部セグメントからサーバーが設置されているセグメントに対する適切なアクセス制御が可能なネットワーク構成がとられているか。外部公開サーバーとして、どのようなものがあるか。不必要なサーバーはないか。
- **A(2)** ルーター又はファイアウォール等でのフィルタリング設定によって、未使用又は不必要なポート／プロトコル／不正なIPアドレスによる接続を排除しているか
- **A(3)** 未使用又は不必要なデーモン／サービス／エージェント／アカウントが全て停止又は削除されているか
- **A(4)** ファイルが格納されている場所のアクセス権が制限されているか
- **A(5)** パスワードの設定に係るルールが適切に定められているか。例えば、システム管理者及びユーザーについて以下の項目が満たされているか
  - 辞書に載っている単語を利用していないこと
  - 人名等固有名詞を利用していないこと
  - IDと同じでないこと
  - 過去に利用したパスワードを再利用していないこと
  - 定期的に変更していること

図10　セキュリティ対策セルフチェックシート　出題チェック項目例 [9]

[9] http://www.ipa.go.jp/security/ciadr/checksheet.html

2. 情報セキュリティ分野以外の自己診断チェックリスト　事例調査結果

2.1. サマリー

情報セキュリティ分野以外の自己診断チェックリストに係る国内の取組事例を取りまとめた。

事例	取組機関	分野	対象	様式		配布媒体		
				段階評価型	クイズ形式	アナログメディア	デジタルメディア	イベントサポータ支援
労働者の疲労蓄積度自己診断チェックリスト	厚生労働省	健康管理	国民	○		○	○	
自己診断疲労度チェックリスト	疲労科学研究所	健康管理	国民	○		○	○	
活用する力を高めるセルフチェックリスト	千葉県教育庁	人材育成	企業	○		○	○	
中小ITベンダー人材育成チェックリスト	IPA	人材育成	企業	○		○	○	
自己診断チェックリスト	日本私立学校振興共済事業団	経営改善	企業	○		○	○	

図 11　情報セキュリティ以外の分野における自己診断チェックリスト　事例調査結果サマリー

2.2. 健康管理

2.2.1 労働者の疲労蓄積度自己診断チェックリスト (厚生労働省)

①作成指針

健康障害防止の視点から、これまでの医学研究の結果などに基づいて、仕事による負担度を判定できるように作成されている。 チェックリスト作成委員会を独自に設けており、チェックの方式，項目，判定方法の検討を行っている 。

②目的対象

労働者を対象に過重労働による健康障害を防止するために、労働者自身に自らの疲労度を把握し、積極的に自己の健康管理を行ってもらうことを目的としている。

③配布方法

厚生労働省のホームページ上(http://www.mhlw.go.jp/topics/2004/06/tp0630-1.html)にチェックリストのリンク先を掲載しており、リンク先の自己診断チェックリストはPDF形式で、自分自身で印刷をかけて利用できるようになっている。ホームページ上に直接問題を記載することはしていない。疲労度を自分自身でチェックできる本人用チェックリストと、客観的に見て相手の疲労度を評価する家族用チェックリストの 2 つを配布している。

図 12 労働者の疲労蓄積度チェックリスト パンフレット表紙イメージ[10]

[10] http://www.mhlw.go.jp/topics/2004/06/dl/tp0630-1d.pdf

④チェックリストの様式

各チェック項目での質問に対して、自分自身の健康状態を3段階で評価形式であり、チェック項目は全20項目で構成されている。所要時間は5分程度である。チェック項目の選択肢には、自己の健康状態に応じて点数が設定されており、総得点で疲労度を判断できるように工夫している。

チェック項目の内容は全て医学的な知見に基づき作成された項目で、チェックリスト利用者の心理面や健康状況を聞くチェック項目と、チェックリスト利用者の生活環境を聞くチェック項目の2つの観点から構成されている。

⑤特記事項

パンフレットには、「労働者の疲労度チェックリスト」だけでなく、家族の視点から労働者の疲労度を評価する家族用チェックリストや、過重労働による健康障害を防ぐための対策や注意事項などを掲載している。

1 最近1か月間の自覚症状について、各質問に対し最も当てはまる項目の□に✓を付けてください。

1. イライラする	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
2. 不安だ	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
3. 落ち着かない	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
4. ゆううつだ	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
5. よく眠れない	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
6. 体の調子が悪い	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
7. 物事に集中できない	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
8. することに間違いが多い	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
9. 仕事中、強い眠気に襲われる	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
10. やる気が出ない	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
11. へとへとだ(運動後を除く)	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
12. 朝、起きた時、ぐったりした疲れを感じる	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)
13. 以前とくらべて、疲れやすい	□ ほとんどない(0)	□ 時々ある(1)	□ よくある(3)

自覚症状の評価 各々の答えの( )内の数字を全て加算してください。 **合計**________ **点**

Ⅰ	0−4点	Ⅱ	5−10点	Ⅲ	11−20点	Ⅳ	21点以上

2 最近1か月間の勤務の状況について、各質問に対し最も当てはまる項目の□に✓を付けてください。

1. 1か月の時間外労働	□ ない又は適当 (0)	□ 多い (1)	□ 非常に多い (3)
2. 不規則な勤務(予定の変更、突然の仕事)	□ 少ない (0)	□ 多い (1)	□ −
3. 出張に伴う負担(頻度・拘束時間・時差など)	□ ない又は小さい (0)	□ 大きい (1)	□ −
4. 深夜勤務に伴う負担(★1)	□ ない又は小さい (0)	□ 大きい (1)	□ 非常に大きい (3)
5. 休憩・仮眠の時間数及び施設	□ 適切である (0)	□ 不適切である (1)	□ −
6. 仕事についての精神的負担	□ 小さい (0)	□ 大きい (1)	□ 非常に大きい (3)
7. 仕事についての身体的負担(★2)	□ 小さい (0)	□ 大きい (1)	□ 非常に大きい (3)

★1:深夜勤務の頻度や時間数などから総合的に判断してください。深夜勤務は、深夜時間帯(午後10時−午前5時)の一部または全部を含む勤務を言います。
★2:肉体的作業や寒冷・暑熱作業などの身体的な面での負担

勤務の状況の評価 各々の答えの( )内の数字を全て加算してください。 **合計**________ **点**

A	0点	B	1−2点	C	3−5点	D	6点以上

【仕事による負担度点数表】

		勤務の状況			
		A	B	C	D
自覚症状	I	0	0	2	4
	II	0	1	3	5
	III	0	2	4	6
	IV	1	3	5	7

※糖尿病や高血圧症等の疾病がある方の場合は判定が正しく行われない可能性があります。

⇨ あなたの仕事による負担度の点数は：□ 点（0～7）

	点 数	仕事による負担度
判定	0～1	低いと考えられる
	2～3	やや高いと考えられる
	4～5	高いと考えられる
	6～7	非常に高いと考えられる

図 13 疲労蓄積度チェックリスト 出題チェック項目例 [11]

[11] http://www.mhlw.go.jp/topics/2004/06/dl/tp0630-1d.pdf

2.2.2　自己診断疲労度チェックリスト　(株式会社疲労科学研究所)

①作成指針

　慢性疲労症候群の診断基準に記載されている身体症状と精神神経症状をもとにチェック項目の内容を精査している。作成されたチェックリストは、健常者 120 名、疲労症候群患者 127 名を対象に本チェックリストの有用性の検証実験も実施され、その有用性が確認されている。

②目的対象

　慢性疲労を自覚していながらも休まず働く人々の健康障害を予防することを目的としている。

③配布方法

　　2005 年 3 月 8 日の朝日新聞の記事(「疲労の謎に、科学が迫る」)として掲載される他に、疲労科学研究所のホームページ上(http://www.fatigue.co.jp/check.htm)に直接記載されている。2011 年 3 月に、ホームページ上でチェックリストを利用できるアプリケーションをホームページ内に導入した。

図 14　自己診断疲労度チェックリスト　朝日新聞　掲載記事イメージ[12]

[12] http://www.fatigue.co.jp/check.html

④チェックリストの様式

チェック項目での質問に対して、自己の疲労度を5段階で評価する形式であり、チェック項目は全20項目で構成されている。所要時間は5分程度である。総得点で疲労度を判断できるように工夫している。

厚生労働省が発表する「疲労蓄積度自己診断チェックリスト」と同様、チェック項目の内容は冒頭でも述べたように全て医学的知見から精査されており、身体的疲労と精神的疲労の2つの観点から構成されている。

◆あなたの健康管理シート

症状の点数: 全くない (0点)　少しある (1点)　まあまあある (2点)
かなりある (3点)　非常に強い (4点)

A.身体的疲労 (各項目0点～4点 x 10項目： 40点満点)

1. 微熱がある
2. 疲れた感じ、だるい感じがある
3. 一晩寝ても疲れがとれない
4. ちょっとした運動や作業でもすごく疲れる)
5. 筋肉痛がある
6. このごろ体に力が入らない
7. リンパ節が腫れている
8. 頭痛、頭重痛がある
9. のどの痛みがある
10. 関節が痛む　**合計点 A(点)**

B.精神的疲労 (各項目0点～4点 x 10項目： 40点満点)

11. よく眠れない
12. ゆううつな気分になる
13. 自分の体調に不安がある
14. 働く意欲がおきない
15. ちょっとしたことが思い出せない
16. まぶしくて目がくらむことがある
17. ぼーっとすることがある
18. 思考力が低下している
19. 集中力が低下している
20. どうしても寝すぎてしまう　**合計点 B (点)**

総合計点 A+B (点)

	安全ゾーン	要注意ゾーン	危険ゾーン
総合的評価 (A+Bの得点)	男性 0～16 女性 0～19	男性 17～22 女性 20～28	男性 23以上 女性 29以上

図15　自己診断疲労度チェックリスト　出題チェック項目例[13]

[13] http://www.fatigue.co.jp/check.html

⑤特記事項

　本チェックリストは「疲労および疲労感の分子・神経メカニズムとその防御に関する研究「慢性疲労症候群に対する治療法の確立」の報告書より抜粋したものである。

2.3. 人材育成

2.3.1 セルフチェックリスト (千葉県教育庁南房総教育事務所)

①作成指針

千葉県教育庁が独自に示した自己診断チェックリストの作成指針を利用している。具体的な作成指針として以下のような観点が挙げられている。

- セルフチェックリスト作成指針
  - ・評価項目は、数を絞り、分かりやすく設計
  - ・項目を具体的にするため、観点の例として説明を付加
  - ・一度だけでなく、継続的、計画的に利活用できるように設計　など

②目的対象

教育者を対象に、問題解決的な授業を充実させ、活用する力が子供たちの間で育つように指導できるスキルを向上させることを目的としている。

③配布方法

パンフレットを作成しており、千葉県のホームページ（http://www.pref.chiba.lg.jp/kyouiku/kj-nanbou/shidoushitsu/index.html）でPDF版を公開している。PDFをダウンロードすることで、パンフレットを紙で配布もできる。

～ 活用する力を高める ～

セルフチェックシート

－ もくじ －

千葉県教育庁南房総教育事務所

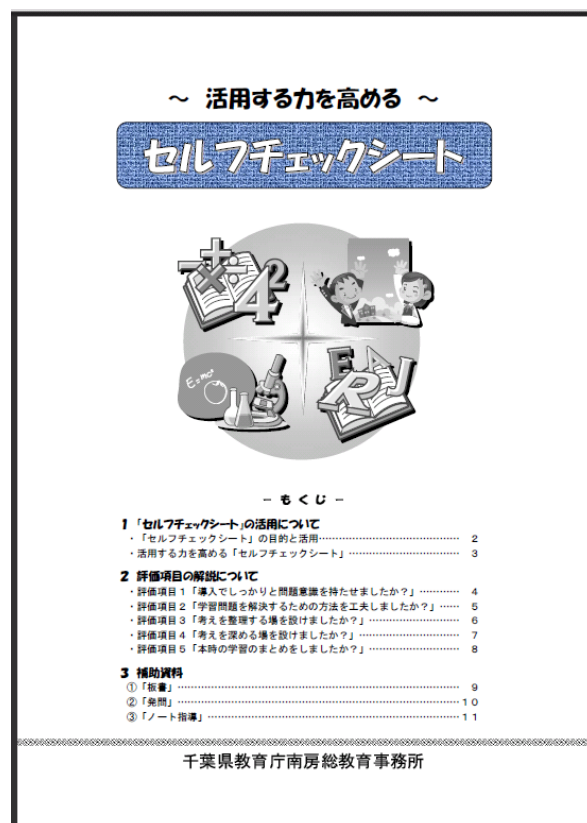



図 16　～活用する力を高める～　セルフチェックリスト　パンフレット表紙イメージ[14]

[14] http://www.pref.chiba.lg.jp/kyouiku/kj-nanbou/shidoushitsu/documents/self.pdf

④チェックリストの様式

各評価項目に対して自分自身の達成度を4段階で評価する形式で、容易に繰り返し利用ができるようにチェック項目数は全5問で構成されている。

チェック項目の内容は、拾行全体での取り組みを網羅的に評価するために、授業の導入から授業中の取り組み(展開)、最後のまとめの3つの段階で構成されている。各チェック項目は短く簡潔に記載されているが、その内容を補足するように、具体的な評価観点も同時に記載されており、個人ごとの診断基準のばらつきを少なくする工夫が図られている。

4：十分できた　3：概ねできた　2：あまりできなかった　1：できなかった			
過程		評　価　項　目	自己評価
導入	1	**導入でしっかりと問題意識を持たせましたか？** ＜観点例＞ ①本時の学習の手助けとなる既習事項を確認した。 ②興味・関心や疑問を持つような資料を提示した。 ③子どもの疑問等を生かした学習問題を作った。	4・3・2・1
展開	2	**学習問題を解決するための方法を工夫しましたか？** ＜観点例＞ ①解決の見通しを持たせた。 ②解決に適した学習形態を工夫した。 ③解決に必要な資料を適切に活用した。	4・3・2・1
	3	**考えを整理する場を設けましたか？** ＜観点例＞ ①考えを整理する時間を確保した。 ②ノート等を活用する指導をした。 ③記録・要約・説明・論述などの言語活動を取り入れた。	4・3・2・1
	4	**考えを深める場を設けましたか？** ＜観点例＞ ①自分の考えを分かりやすく説明する指導をした。 ②話し合い活動を取り入れた。 ③話し合い活動の中で，自分の考えを深める指導をした。	4・3・2・1
まとめ	5	**本時の学習のまとめをしましたか？** ＜観点例＞ ①学習したことが身に付いたかを確認した。 ②自己評価や相互評価などの評価活動を行った。 ③新たな問題を発見するなど，学習への関心や意欲を持たせた。	4・3・2・1

図17　～活用する力を高める～　セルフチェックリスト　チェック項目例[15]

[15] http://www.pref.chiba.lg.jp/kyouiku/kj-nanbou/shidoushitsu/documents/self.pdf

⑤特記事項

各評価項目を自己診断する際の観点に対して、補足資料として１項目につきA4で１枚パンフレットの中に記載されている。 具体的には、チェック項目１の観点①を例に上げると、「本時の学習の助けとなる既存事項を確認したか？」に対して、既存事項の確認が意味することは何かを記載し、その確認方法も合わせて分かるように記載している。

2 評価項目の解説について

評価項目１

導入でしっかりと問題意識を持たせましたか？

＜観点例＞
① 本時の学習の手助けとなる既習事項を確認した。
② 興味・関心や疑問を持つような資料を提示した。
③ 子どもの疑問等を生かした学習問題を作った。

１時間の授業の導入においては，子どもたちに，興味・関心を持たせ，学習意欲を促すことが必要です。そのためには，導入の工夫，資料提示の工夫をすることにより，この単元で，今日の授業で，「どんなことを学習するのか」という問題意識を持たせることが何よりも大切です。

■観点①　既習事項の確認

既習事項の確認としては，
○前時までの既習事項の確認
○前学年までの既習事項の確認

特に中学校では，小学校の段階ではどこまで学習しているのか，把握しておきましょう。

既習事項の確認の方法としては，プレテストやアンケート等による調査が一般的です。そして，教師の日常の観察による実態把握が重要であることは言うまでもありません。

■観点②　資料提示と発問

ア　資料提示の工夫

子どもたちに興味・関心，疑問や問題意識を持たせるためには，資料提示の工夫が大切です。

その方法には，
○教科書，資料集，副読本，書物，新聞
○文章や絵，写真，調査統計表
○具体物や実物
○ペープサート
○OHPやスライド，パソコン
○テレビやビデオ
○役割演技や体験活動

の活用などがあります。内容や目的に応じて，これらを選んだり組み合わせたりして工夫しましょう。また，全てを提示しないで，一部を隠したりする（マスキング）などの手法もよく使われます。

イ　発問の工夫

資料や素材を提示する時に大事なのが，教師の発問です。発問の如何によって，子どもたちの興味・関心や疑問が変わってしまうこともよくあります。

「この絵から気づいたことは何ですか。」
「何をしている写真でしょう。」
「隠れている部分は何でしょう。」
「この人は何を考えているのでしょう。」
「この題名からどんなことを考えますか」

時には，黙って提示して，「あれっ？」と思わせることも効果的です。

■観点③　よい学習問題の条件

多くの授業において「学習問題」が設定されます。しかしながら，その学習問題が，ねらいに迫るものでない場合も見られます。

よい学習問題の条件として，
○学習のねらいに到達できるもの
○子どもの意欲を喚起するもの
○子どもの問題意識に支えられているもの
○子どもなりの予想が立てられるもの
○調べ方，追究方法がわかるもの

などが挙げられます。また，具体例として，
①活動型「～について探ろう」
②確認型「どんな特色があるだろう」
③思考型「なぜだろう」

があります。資料提示を工夫し，発問を吟味し，子どもたちが学ぶ意欲を持つ学習問題づくりが重要です。

図 18　～活用する力を高める～　セルフチェックリスト　観点の解説イメージ[16]

[16]http://www.pref.chiba.lg.jp/kyouiku/kj-nanbou/shidoushitsu/documents/self.pdf

2.3.2　中小 IT ベンダ人材育成　チェックリスト　(独立行政法人　情報処理推進機構)

①作成指針

「高度IT人材こそがIT企業の経営力の源泉である」と考え、IT企業が何らか気づきを得て欲しい、より良い企業経営に繋げて欲しいという思いから、IT人材育成の取り組みを評価するツールとしてチェックリストが作成されている。

②目的対象

自社の人材育成に対する取り組み状況を自己評価し、IPA が実施する「中小 IT ベンダ人材育成優秀賞※」への応募を判断できるように作成した。

※中小 IT ベンダにおいて、経営戦略に即した IT 人材育成の取り組みを組織的に実践し、その取り組みが IT 業界の産業構造の変革に対応しており、企業組織全体が活性化されている企業を表彰する制度

③配布方法

IPAのホームページ上(http://www.ipa.go.jp/jinzai/award/vendor2011/application.html#files)からPDF形式とエクセル形式で公開している。PDFおよびエクセルをダウンロードすることで、紙媒体での配布も可能である。

④チェックリストの様式

チェック項目は、質問に対して自社の取り組み状況を 3 段階で評価する形式であり、チェック項目数は全 10 問、解答所要時間は 20 分程度である。

企業の人材育成への取り組みを公式的に提出しなければならないため、いずれの選択肢も非常に具体的な内容が記載されており、自社の取り組みの現状を明確に判断することができる。

・　人材が持っている知識やスキルなど、能力のレベルを測定し、高めていく仕組みがありますか？
また、それは社員の多くが活用するほど機能していますか？

□ レベル 1

人材像に基づく育成サイクルについてスキル標準に準拠したアセスメントは不定期に実施しているが、教育研修への連動や社内認定などの仕組みは動いていない

何らかの形でスキル標準のアセスメントを行ったが、個人別育成PDCAサイクル確立までには至っていない状態

□ レベル 2

企業として求める人材像の明確な定義は無いが、スキル標準を活用した必要レベルの定義はあり、教育ロードマップにも連動させている

何らかの形でスキル標準のアセスメントを行い、これを起点とした個人別育成PDCAサイクルがどのようなレベルであれ存在はするが、CAが弱い状態

□ レベル 3

企業として求める人材像と、それに対応させた要件が、スキル標準やコンピテンシーを用いて定義されており、若手・中堅の成長目標となっている

経営目標とリンクした人材像がスキル標準とコンピテンシーで定義され、これを起点とする個人別育成PDCAサイクルが確立され制度としてきちんと運用されている状態

図 19　中小ITベンダ人材育成　チェックリスト　チェック項目例　(1/2)[17]

[17] http://www.ipa.go.jp/jinzai/award/vendor2011/doc/a3_check.pdf

・ 人材が持っている知識やスキルなど、能力のレベルを測定し、高めていく仕組みがありますか？また、それは社員の多くが活用するほど機能していますか？

□ レベル 1

技術的専門分野の教育研修は受講されているが、ビジネススキルや人間力に対応したものは殆ど受講機会が無い

テクニカルスキル開発や資格取得といった短期的な視点による教育提供に留まっている状態。社会人基礎力など業務に必要な人間教育の視点は薄い

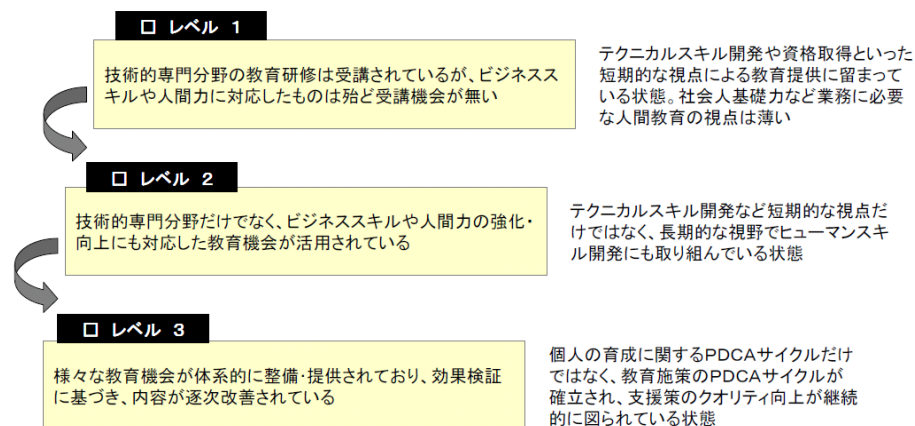
□ レベル 2

技術的専門分野だけでなく、ビジネススキルや人間力の強化・向上にも対応した教育機会が活用されている

テクニカルスキル開発など短期的な視点だけではなく、長期的な視野でヒューマンスキル開発にも取り組んでいる状態

□ レベル 3

様々な教育機会が体系的に整備・提供されており、効果検証に基づき、内容が逐次改善されている

個人の育成に関するPDCAサイクルだけではなく、教育施策のPDCAサイクルが確立され、支援策のクオリティ向上が継続的に図られている状態

・ 社員の側から手を挙げて何か（新しい仕事や学習のための機会）に挑戦できるような仕組みがありますか？また、それは多くの職場で機能しているでしょうか？

□ レベル 1

社員からの声を聞いたり、自己申告を受け付けてチャレンジの機会を与えていくような、公式の仕組みは無く、必要性も議論されていない

人材マネジメントを経営に生かそうとする視点が無い状態。

□ レベル 2

社員が今後取り組んでみたい仕事や働いてみたい職場などの希望を定期的に自己申告する仕組みはあるが、希望がかなう例は未だ多くない

一応双方向の自己申告制度はあるが、運用が不十分な状態

□ レベル 3

自己申告制度について、その実績から希望に沿うかそれに近い形での異動や学習機会の提供がなされていると、社内で広く認知されている

社員側に自己申告制度を活用し、キャリア開発の契機にしようとする意思と信頼感があり、経営もこの希望をかなえることで活性化による新事業創出や生産性向上など、経営成果に結び付けようとする意図があり、これを実現する制度が健全に機能している状態

図 20　中小ITベンダ人材育成　チェックリスト　チェック項目例　(2/2)[18]

[18] http://www.ipa.go.jp/jinzai/award/vendor2011/doc/a3_check.pdf

2.4.　経営改善

2.4.1　自己診断チェックリスト　平成 23 年度版(日本私立学校振興・共済事業団　科学振興事業本部)

①作成指針

学校法人の経営者を対象に、管理運営上問題となる定性的要因に関する設問を共済事業団で設定し、学校法人が本来実施していなければならないポイントを要点として記載する。

②目的対象

本チェックリストを用いて、学校法人が自ら経営状況を分析し、問題が見つかれば自主的な改善努力への誘因となることを目的としている。

③配布方法

私学振興事業本部のホームページ上(http://www.shigaku.go.jp/s_center_checklist23.htm)からPDF形式とエクセル形式で公開している。PDFおよびエクセルをダウンロードすることで、紙媒体での配布も可能である。

④チェックリストの様式

チェック項目は、自社の経営状況に関する 8 つの観点(後述)からの取り組み状況を、Yes/No 形式で解答する形式であり、チェック項目数は全 50 問で構成されている。　解答が No のチェック項目の取り組み状況を再度確認することで、現状の課題と解決策への糸口を見つけ出すことが可能となる。

チェック項目の内容は、作成指針に記載した内容と重複するので割愛する。

- 経営状況に関する 8 つの観点
  1) 経営理念と戦略の策定
  2) ガバナンスの確立
  3) 組織運営の円滑化
  4) 危機管理体制の構築
  5) 財務体質の改善
  6) 教学内容の改善
  7) 学生への支援
  8) 情報公開と発信

1. 経営理念と戦略の策定	1	建学の精神を、時代に即した使命として確立し、全部門に明示しているか
	2	建学の精神を踏まえた経営戦略を策定しているか
	3	全学の総意により、中長期計画・経営戦略等を策定しているか
	4	経営環境（内部・外部）と経営資源（ヒト・モノ・カネ等）の変化を分析し、経営戦略に反映しているか
	5	中長期計画の進捗度を定期的に把握し、結果の評価や見直しを行っているか
2. ガバナンスの確立	6	理事長を中心とする理事会が学校法人の最終的な決定機関として機能しているか
	7	一部の理事に権限が集中し、理事会の一体的な協力体制が損なわれていないか
	8	外部理事や評議員会から経営者に対する適切な助言とチェックが行われているか
	9	理事会の決定方針は、全部門・全教職員に周知徹底されているか
	10	財務だけでなく学校法人の運営全般について監事の監査機能は十分に果たされているか
	11	業務が法令、規程に基づいて適正に行われていることを自らチェックするための内部統制組織を整えているか
	12	公認会計士の指摘や助言を活用し、必要な改善策を立てているか
	13	経営方針を企画立案し、連絡調整等を行う組織を設置しているか
	14	資産運用規程の整備等、時機に即した規程の整備・見直しを行い、規程にのっとった運営を行っているか
	15	使途不明・不正流用・二重帳簿作成などの不適正な会計処理が生じないように、十分なチェックが行われているか
	16	経営者及び教職員は、学校法人の会計と財務の仕組みを十分理解しているか
	17	経営者は教職員に対して自法人の財務状況を毎期十分に説明する機会を設けているか
3. 組織運営の円滑化	18	教職員からの意見を反映させる仕組みや業務分担が機能しているか
	19	アウトソーシングの活用や組織体制の見直し等により、事務組織が有効に機能し、効率的な職務体制となっているか
	20	労働組合に十分な情報提供と説明を行い、適切な労使関係が構築されているか
	21	教職員に対する研修を計画的に実施し、研修成果の検証をしているか
	22	人事考課を行っている場合、評価の基準、評価方法、評価結果の活用等について、見直しと改善が進められているか

図 21　自己診断チェックリスト　チェック項目例 [19]

[19]http://www.shigaku.go.jp/files/s_center_checklist23-kaisetsu.pdf

3.　高齢者向け資料　事例調査結果

3.1.　サマリー

高齢者向け普及啓発に係る国内の取組事例を取りまとめた。

※1　インターネットを介さない配布媒体
※2　インターネットを介した配布媒体

事例	取組機関	分野	対象	配布媒体		
				アナログメディア※1	デジタルメディア※2	イベントサポータ支援
NECシニアITサポータ養成講座	NEC	情報セキュリティ	高齢者	○	○	○
地上デジタル放送関連取り組み	総務省	地上デジタル放送	国民	○	○	○
振り込め詐欺関連取り組み	警察庁 その他関係機関	振り込め詐欺	高齢者	○	○	○
高齢者のための、やさしい安全・安心ハンドブック	東京都港区	振り込め詐欺	高齢者	○	○	

図 22　高齢者向け資料　事例調査結果　サマリー

3.2.　NECシニアITサポータ養成講座　(NEC)

①目的対象

シニア IT サポータ養成講座は、IT スキルを持っているシニア世代の方を中心に、障害者や高齢者のパソコン活用を支援する「IT サポータ」を養成することを目的としている 。地域社会の中で IT サポータとして活躍できる人材が増えることで、地域社会内での高齢者間における IT の普及啓発活動が促進されることが考えられる。

②配布方法

NPO などの各地の団体と協働でイベントを開催し、講座を行う。2008 年度末までに講座修了生は 1000 名を越えており、多くの IT サポータが世に輩出されている。

講座は、計 2 日、それぞれ 5 時間程度のプログラムで構成されている。

③高齢者向け資料の様式

内容は開催地域でそれぞれであるが、主には IT サポータの役割と IT サポータに必要なスキルを学ぶ場となっている。講座の内容の例を以下に挙げる。

- NEC シニア IT サポータ養成講座　講義内容例
  - ・スキルアップ講座
  - ・サポート実例集
  - ・Vista の使用方法
  - ・Windows ユーザー設定方法
  - ・よくあるインターネットのトラブルとチェックポイント
  - ・インターネットとホームページのしくみ
  - ・キーボードショートカットの使い方
  - ・ウェブ・アクセシビリティ支援ツール体験 ・WebUD

図 23　NECシニアITサポータ養成講座　講義イメージ [20]

[20] http://www.nec.co.jp/community/ja/it/elderly.html

3.3.　地上デジタル放送関連取り組み　(総務省)

①目的対象

全国民を対象に、2011 年 7 月までに完全移行が予定されていた地上デジタル放送への完全移行を達成することを目的としている。

②普及啓発実施方法

普及啓発実施方法は多岐に亘り、TVCM、新聞、中刷り広告、雑誌、ポスター、看板、パンフレットなどのアナログ媒体やインターネット広告などのデジタル媒体が複合的に活用された。また、キャンペーン活動などのイベントも実施され、地上デジタル放送への移行を国民へ呼び掛けたり、地上デジタル放送への移行手続きの説明などを実施していた。“地デジカ”が愛称のキャンペーンキャラクターなども製作している。

地上デジタル放送へと移行が完了していない高齢者世帯に個別に訪問して、地上デジタル放送への移行に関する説明やアドバイスも無料で行っている例も散見された。

③地上デジタル放送への完全移行推進に要する予算額

地上デジタル放送のメリットなどについて国民への情報提供活動に要した金額の概算を以下に示す。

- 地上デジタル放送への完全移行推進に要する予算額
  - ・2002 年度：1.5 億円
  - ・2009 年度：5.3 億円
  - ・2010 年度：8.4 億円

3.4.　振り込め詐欺関連取り組み　(警視庁　その他関係機関)

①目的対象
　全国民を対象とした、振り込め詐欺を防止するための活動である。

②普及啓発実施方法
　TVCM や新聞、雑誌、中刷り広告、看板、ポスター、パンフレットなどのアナログ媒体や、インターネット広告などのデジタル媒体が複合的に活用されている。振り込め詐欺への注意を呼び掛けるイベントも多く存在し、講義形式のものから直接家に訪問し振り込め詐欺の危険性の説明を行いポスターを配布するなどの訪問形式の活動も実施されている。
　体制面に関して、軽視庁や道府県警察本部では、振り込め詐欺対策本部を設置している。対策本部では、国民が詐欺の手口や事例を周知できるように、ホームページ上にそれらの情報を公開したり、紙媒体で配布するなどの普及啓発活動を実施している。警察関係機関だけでなく、マスコミや金融機関、地方自治体からも振り込め詐欺の注意喚起がされている。
　法律面では、被害の性質を考慮することができる「振り込め詐欺救済法」が制定されるなど、国民の振り込め詐欺の被害を軽減する措置が図られている。

③振り込め詐欺への取り組みに要する予算額
　犯罪対策関連経費として 2010 年度の予算額は 200 万円程度であった。

3.5.　高齢者のため、やさしい　安全・安心ハンドブック　(東京都港区)

①目的対象

高齢者を対象に、高齢者の大切な“命”と“財産”を守るために「高齢者のための、やさしい　安全・安心ハンドブック」が東京都港区で配布されている。

②配布方法

東京都港区でパンフレットとして配布されている他に、港区のポータルサイトから同資料のPDF形式を閲覧およびダウンロードすることが可能となっている。

③高齢者向け資料の形式

「高齢者のための、やさしい　安全・安心ハンドブック」は以下の6つのテーマから構成されており、その1テーマとして振り込め詐欺に関する注意喚起がされている。

- 安全・安心ハンドブックで扱う6つのテーマ
  - ・住宅の侵入に備える
  - ・街頭での犯罪に備える
  - ・乗り物盗・車上狙いに備える
  - ・振り込め詐欺に備える
  - ・悪質商法に備える
  - ・交通事故に備える

パンフレット全体を通して、文字のフォントは14ポイント以上の大きさで記載されていて、高齢者でも読みやすい文字サイズになっている。特に強調したいフレーズに関しては50ポイント以上となっている。

振り込め詐欺のテーマは以下の4つの小項目から構成されている

- 「振り込め詐欺」で説明される4つの小項目
  - ・振り込め詐欺の種類
  - ・撃退方法
  - ・ケーススタディ
  - ・振り込め詐欺に備える
  - ・その他ケースの紹介

イラストを用いることで、振り込め詐欺の1場面がイメージできるように工夫がされている[21]。

[21] http://www.city.minato.tokyo.jp/kurasi/iza/bosai/anzen/koureianzen/index.html

別添資料 6

海外事例集

2012年3月

株式会社 NTT データ経営研究所

目次

1. サマリー

自己診断チェックリストおよび高齢者向け普及啓発に係る海外 5 カ国の取組事例を取りまとめた。

国	名称	対象	様式：段階評価型	様式：クイズ形式	配布媒体：アナログメディア※1	配布媒体：デジタルメディア※2	配布媒体：イベントサポータ支援
アメリカ合衆国	ミシガン州サイバー戦略ツールキット	国民		○		○	
	Cyber Secutity Control Checklist	企業	○			○	
	高齢者用インターネット安全	高齢者	冊子			○	
	貯蓄上手なシニア	高齢者		○		○	○
英国	Protect My ID	国民	○			○	
	Personal Security Checklist	国民		○		○	
	インターネットを活用するインターネット安全性	高齢者	冊子			○	
ドイツ	ITセキュリティガイドライン	企業	○			○	
	ネットでの安全　－ITセキュリティ	国民		○		○	
	50歳以上をネットワークへ	高齢者	冊子		○	○	○
	誰だか当ててみて　－詐欺師と泥棒の手口から身を守るには	高齢者	冊子		○	○	○
スウェーデン	サーフカム	国民		○		○	
	ヨーテボリ市ITガイドライン	企業		○	○	○	
	ACTION	高齢者	対話型サービス			○	○
シンガポール	ファースン・アップ	国民		○		○	
	サイバロニア	こども		○		○	
	シルバー・インフォコム	高齢者	冊子			○	○

※1　インターネットを介さない配布媒体
※2　インターネットを介した配布媒体

2. アメリカ合衆国

2.1. ミシガン州サイバー戦略ツールキットMichigan Cyber Initiative Toolkit

①目的・対象

ミシガン州の市民、ビジネス、政府機関を幅広く対象とした、サイバーセキュリティに関する取り組み(Michigan Cyber Initiative)である 。
本取組は、ウェブサイト(http://www.michigan.gov/cybersecurity) に掲載されている資料をダウンロードまたは印刷し、ミシガン州市民とその家族、職場の同僚や、コミュニティに配布することで、情報セキュリティの理解・認識を高め、実践させることを狙いとしている。

②提供方法

インターネットによる公開型で、無料でダウンロードが可能。ダウンロードや印刷は市民が各自で行う。アメリカでは毎年 10 月がサイバーセキュリティー啓発月間と定められている。[1]サイバーサミットが 2011 年 10 月 7 日に東ミシガン大学で開催された。ミシガン州は、サイバーセキュリティに関しては他州をリードすると自負している通り、州内での認識・理解の向上を積極的に促している。[2]

③様式・内容

ツールキットには、以下の 4 種のコンテンツが含まれる。

(1) サイバーセキュリティークイズ (4 種類)[3]
4 種類のクイズが紹介されている。うち 3 つは、外部の民間組織により提供されており、リンクをクリックすると、それぞれ括弧内に示す組織の運営するウェブページが開く。

・ミシガン州オンラインセキュリティクイズ：General Quiz 1、General Quiz 2 (いずれもセキュリティに関する用語や、危険回避のための基本的な対処法を問う問題)、At Home (家庭で起こりうる危険への対処法)、Advanced Quiz (危険回避のために有効なソフトウェアなど技術的な内容) の 4 種類があり、それぞれ 5～13 問の選択式の問題で構成されている。（図 1.1.1）

・フィッシングクイズ(Contents Verification)：正誤式の 9 問により構成されている。

・フィッシング IQ クイズ(Mail Frontier)：3 択問題 10 問により構成されている。

・個人情報セキュリティクイズ(Better Business Bureau)：リンクは存在するが、エラーのため内容を確認できなかった。

図 1.1.1：サイバーセキュリティクイズ（At Home）のサンプル

[1] http://www.dhs.gov/files/programs/gc_1158611596104.shtm (07/01/2012)
[2] http://events.esd.org/ (17/01/2012)
[3] http://www.michigan.gov/cybersecurity/0,4557,7-217-51788-192552--,00.html (07/01/2012)

Category: At Home
Change category

Your current score: 0 / 0	This question score: 100
Question 1 : What is the name for a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document?	
○ Spyware. ○ Virus. ○ Firewall. ○ Norton.	
	Next >

Total Number of questions for this category: 10

(2) ポスター (3 種類の PDF)
サイバーセキュリティの推進を訴える内容のポスターが用意されている（図 1.1.2）。

図 1.1.2：ポスターの一例

(3) パンフレット (5 種類の PDF)
パンフレットは 5 種類用意されているうち、ひとつは、IT セキュリティに関する子供が描いた絵を用いたサイバーセキュリティカレンダーであった。

(4) ガイドブック（4 種類のオンラインガイドと 6 種類の PDF）および助言集（Tip sheet）
(7 種類)
ガイドブックには、学校、ビジネス、政府、家庭向けの 4 種類があり、それぞれ焦点の異なるサイバーセキュリティ対策が項目ごとにまとめられている。

チップシートには、フィッシング、個人情報の漏洩、ネット上での誹謗中傷など、それぞれの危険を回避するための助言がチェックリスト形式でまとめられている。

一方、ビジネス向けにはニューヨーク州作成の『情報セキュリティ開始－エグゼクティブ、マネージャー向けガイド(Getting Started Guide　PDF)』もダウンロードでき、その中には「ビジネス用情報セキュリティタスク・チェックリスト(p.14) が含まれている。[4]

このほか、同サイトには市民（Citizens）、ビジネス、政府(公務員)向けのページが別に用意されており、各ページにはそれぞれを対象にした内容が盛り込まれている。

- 市民向け：家庭でのサイバーセキュリティの基礎、子供を守る、個人情報漏洩による成りすまし&インターネット詐欺に関する情報と対処法の他、安全を保つためのアドバイスとアンチウィルスソフトなどの紹介。
- ビジネス向け：アクセスコントロール、ビジネス継続性、データの機密性に応じた分類、物理的な安全性、運営マネジメント、法規制遵守について、情報提供や助言をしている。

サイバーセキュリティ関係の資料タイトルをホームページ1枚に纏めることによって、わかり易く効率的に配布、普及できる。ミシガン州以外の団体（中央政府を含む）が作成した資料もいくつか含まれており多様性があるので、市民側の選択する自由度が大きい。

また、文章による説明の他、ビデオを用いて視覚に訴えるコンテンツも含まれている（図1.3）。

図 1.1.3："Cyber Security Videos - Protect Yourself" イメージ

30秒ほどの短いビデオで、ネズミがマウスをいじり、コンピューター画面に猫が写り驚くという比喩を効かせたもの。（http://www.michigan.gov/cybersecurity/0,4557,7-217-34396-153715--,00.html）

[4] http://www.michigan.gov/documents/cybersecurity/Getting_Started_Guide2010_293885_7.pdf (07/01/2012)

2.2. Cyber Security Controls Checklist

①目的・対象

ユタ州のビジネスを対象としている。

ユタ州公共安全局（Departmenr of Public Security）のHomeland Security部門は、"Be Ready Utah"と称される、自然災害や人的被害などの緊急事態からビジネス、家庭、コミュニティを守るため、日頃から十分な準備を推奨している。[5]ソルトレイクシティを擁するユタ州にとって、ビジネスの継続は、州の経済の安定した繁栄を支えるために不可欠である。Cyber Security Controls Checklist は、この取り組みの一環として、不測の災害事態にもビジネス、ならびに顧客や広く一般市民が危険に晒されることがないよう、組織や企業において推奨されるサイバーセキュリティ管理の普及を促す目的で設けられている。同チェックリストに回答することで、回答者は推奨される基本的なサイバーセキュリティ管理のあり方（政策、基準、手続き）を確認し、自社における導入水準を認識することができる。さらに、同チェックリストは、推奨されるセキュリティ管理を文書化する助けとなる。サイバーセキュリティに関する 認識と理解の向上を目的としたものである。

②提供方法

サイバーセキュリティコントロールチェックリストは、"Be Ready Utah" のウェブサイト[6]より無料でダウンロードが可能。

また、"Be Ready Utah" キャンペーンの一部である、不測の事態に備えビジネスの継続性を高める"Ready Your Business" というプロジェクトでは、ビジネスが、人々の生活を揺るがす予期せぬ自然災害や人的被害に備えるための様々なツールキットを提供している。サイバーセキュリティコントロールチェックリストは、同プロジェクトのパートナー組織に配布される"Business Continuity Planning Guidebook"（全 81 ページ）[7]にて掲げられている「事業継続計画のための 12 のプログラム」のひとつにも数えられている。チェックリストは、"Ready Your Business" のワークショップ等でも配布されていると考えられる。

③様式・内容

チェックリストは、以下のサイトに記載されている。http://beready.utah.gov/beready/business/documents/BRUCyberSecurityChecklist.pdf

(1) サイバーセキュリティ・コントロール・チェックリスト

4 ページ全 57 問に渡る質問は、全て Yes/No 選択方式で、以下の 7 項目に分かれている。
- 職員のセキュリティ (Personnel Security)
- 物理的セキュリティー (Physical Security)
- アカウントとパスワード管理 (Account and Password Management)
- 機密性と極秘データ (Confidentiality of Sensitive Data)
- 災害復旧 (Disaster Recovery)
- セキュリティー認識と教育 (Security Awareness and Education)
- コンプライアンスと監査 (Compliance and Audit)

---

[5] http://beready.utah.gov/beready/about.html (08/01/2012)
[6] http://beready.utah.gov/beready/business/ (08/01/2012)
[7] http://beready.utah.gov/beready/business/documents/RYB-BCP2009Guidebook.pdf (08/01/2012)

質問はすべて、推奨されるセキュリティ管理のあり方の有無を尋ねるもので、回答が Yes であれば危険性が少ないと判断される。(図 1.2.1)

図 1.2.1：サイバーセキュリティ・コントロール・チェックリスト（イメージ）

CYBER SECURITY CONTROLS CHECKLIST

This is a simple checklist designed to identify and document the existence and status for a recommended basic set of cyber security controls (policies, standards, and procedures) for an organization. Security controls are designed to reduce and/or eliminate the identified threat/vulnerabilities that place an organization at risk.

PERSONELL SECURITY	Yes	No
1. Does your staff wear ID badges?	○	○
2. Is a current picture part of the ID badge?	○	○
3. Are authorized access levels and type (employee, contractor, visitor) identified on the Badge?	○	○
4. Do you check the credentials of external contractors?	○	○
5. Do you have policies addressing background checks for employees and contractors?	○	○
6. Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?	○	○

(2) サイバーセキュリティ脅威と脆弱性の評価

評価パートは、解説とチェックリストに分かれており、それぞれの内容は以下の通りである。

[解説]

脅威は自然（災害）、人的（テロ、詐欺、ハッキング他）、環境（長期停電や汚染など）の 3 種類に分類される。脅威と脆弱性を判明し、評価することで、組織に潜む潜在的な危険を明らかにすることができる。

危険は、以下の等式で表すことができる。

危険度 = 影響力 × 起こりうる可能性(Risk = Impact × Likelihood)

[チェックリスト (6 頁)]

影響力(0～6 段階)、起こりうる可能性(0～5 段階)を記入し危険度のスコアを計算。スコアから、組織が直面する危険度を高、中、低の 3 段階に分類される。チェックリストは以下の項目ごとに影響力、可能性から危険度を計算する。

- 人的脅威：（ヒューマンエラー、不正など）12 点
- 一般的な脅威：（コンピューターの無許可使用、データの混在、無許可ソフト・ハードウェアの導入など）10 点
- 身分証明承認に関する脅威：5 点
- プライバシーに関する脅威：7 点
- 整合性（インテグリティ）または正確性における脅威：3 点
- アクセスコントロールにおける脅威：8 点
- 拒否に関する脅威（機密情報の取り扱いを行っている事実を認めない、機密情報の情報源を明らかにしない）2 点

- 法的脅威：3 点
- サービスの信頼性に関する脅威：14 点

図 1.2.2：サイバーセキュリティ脅威と脆弱性の評価に使われるチェックリスト

LEGAL THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
1. Failure to comply with regulatory or legal requirements (ie, to protect confidentiality of employee data)	☐	☐	☐
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (ie, incitement to racism, gambling, money laundering, distribution of pornographic or violent material)	☐	☐	☐
3. Liability for damages if an internal user attacks other sites.	☐	☐	☐
RELIABILITY OF SERVICE THREATS	**Impact (0-6)**	**Probability (0-5)**	**Total (Impact x Probability)**
1. Major natural disasters, fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power outages, etc	☐	☐	☐
2. Minor natural disasters, of short duration, or causing little damage	☐	☐	☐
3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.	☐	☐	☐

(3) 推奨されるセキュリティリスク改善行動の例
16 項目の改善行動をとった場合のコスト、恩恵、危険を「低」から「高」で示している。

ビジネス向けのツールであり、内容は簡素で装飾などは一切ない。また、専門用語の解説などもない。企業であれば IT や総務部門の担当者の使用を想定したものと考えられる。組織の安全な運営のための戦略策定にも役立てることができる。

2.3.　高齢者用インターネット安全　Seniors Internet Safety

①目的・対象

ワシントン州司法局（Washington State Office of the Attorney General） は、インターネットの安全性の向上には、まずインターネットの危険性の基本的理解が必要であるとし、今日のインターネット環境に潜む危険分子の理解を促すための情報をウェブサイトにて提供している。情報は、大人(Adults)、家族及び教育者(Families & Educators)、高齢者(Seniors)、若者(Teens) の異なる４つの対象に向け、それぞれ違った切り口でまとめられている。以下、高齢者向けと家族及び教育者向けの内容に焦点を置き紹介する。

② 提供方法

ワシントン州司法局のウェブサイト上で情報提供されている。無料で閲覧が可能。

③様式・内容

(1) 高齢者向けのページ[8](図 1.3.1)

高齢者向けページでは、まず人に出会う、ビジネスを行う、旅行計画を立てる、記録の閲覧、友人や家族と連絡を取り合う、趣味や興味を支援するなど、インターネットが高齢者にもたらす利便性を記している。その上で、高齢者を食い物にする輩の餌食になることなしに、このような機会を享受する方法 (how to take advantage of the opportunities without falling prey to predators so you can have peace of mind when you go online) を学んで欲しいと冒頭で述べることで、インターネットの光と影の部分を強調している。

図 1.3.1: 高齢者向けのトップページ

[8] http://www.atg.wa.gov/InternetSafety/Seniors.aspx (13/01/2012)

内容が多岐に渡る大人向けのページに対し、高齢者向けのページは、高齢者が陥りやすい以下の各項目に絞って構成されている。説明もより丁寧かつ簡潔で、インターネット初心者を意識してわかりやすく表記されている。

高齢者向けページの内容

- 特に高齢者の危険を高める要因

インターネット上での危険性は世代を問わず存在するが、高齢者に顕著な危険因子として、「コンピューター技術の欠乏」、「インターネット利用技術の欠乏」、「信じやすさ」を挙げている。特に「信じやすさ」については、高齢者は豊富な人生経験で他人の判断する能力が培われていることを肯定する一方、若者と比較し公的文書と見受けられる資料（official looking materials ）を信用しやすいこと、また被害が発覚することで自身の名声を汚す可能性を嫌う傾向があることなど、高齢者ならではの性質が仇となりうることを指摘している。

- ソーシャルネットワークサイト

高齢者対象の SNS サイトは、健康状態や財産など個人的な情報を聞き出すクイズやアンケートの対象となりやすい。個人情報の提供には十分な配慮をすることを喚起している。

- サイバーいじめ（誹謗中傷）

特に家族の一員から、感情的な攻撃や、高齢者の財産の濫用目的で、面と向かってではなくインターネット上で攻撃を受ける可能性を示唆している。

- 出会い系サイト

離婚や死別によりパートナーを失った高齢者にとって、出会い系サイトは人と出会う有効な手段である一方、犯罪者にとっては獲物を探すための絶好の機会である（a way predators to find potential victims）。長年連れ添ったパートナーを失って寂しい高齢者は格好の餌食となってしまうと注意を促している。

- 情報暴露

高齢者に見られがちな、インターネットでの情報開示に関する誤解 3 点 (1. 自分がコンピュータを使わなければオンラインに自分の情報が流れることはない、2. Scam 被害に引っかかっていなければインターネット犯罪の被害に遭うことはない、3. 自分がオンラインに投稿した情報は自分のことを知る人にしか閲覧されない) を指摘し、注意を促す。

- 高齢者向けオンラインでの安全に関する助言

最後に、オンラインで自己の安全を保持するための助言が 8 点列挙されている。これらは特に高齢者に限って該当するものではなく、一般的な内容である。

(2) 家族及び教育者向けのページ[9]

「インターネット上で家族の安全を守る」ためのチェックリストが掲載されている。チェックリストは全 14 項目により構成されている。中には、「セイフティソフトウェア等のツールを導入する」、「家族や友人とオンラインでの安全性を守るための対策を話し合う」、「子供がいる場合、コンピューターは家の中の目に付く場所に置き使用する」、「定期的に家族でインターネットの使用やオンラインでの活動を話し合う」等、子供や高齢者を含めた家族ぐるみでの取り組みが推奨されている。

[9] http://www.atg.wa.gov/InternetSafety/FamiliesAndEducators.aspx (12/01/2012)

また、インターネットの使用に関する家庭内でのルール設定を助けるため、家族向けの「インターネット安全性に関する誓約書」（Internet safety contract for families ）をサンプルとして紹介している。同サンプル誓約書は 10 項目からなり、子供が署名するように作られているが、その内容は大人や高齢者のインターネット利用に対しても有効と思われるものである（図 1.3.2）。

また、画面右側の Internet Safety Topics にある各項目は、世代間共通で利用できるようにサイトが構成されている。PDF など紙媒体の配付はない。

図 1.3.2: 家族向け「インターネット安全性に関する誓約書」

（Internet safety contract for families）

Internet safety contract for families

The Internet is a public place and I am responsible for using it safely to help protect myself, my family, and my friends.

- I will only use safe contact names—in e-mail, IM, blogs, etc.
- I will never use the Internet to bully or harass anyone.
- I will not post content to a public site without my parent's permission.
- I will not expose my personal information or the information of my friends or family (name, address, phone or cell numbers, school) in text or through pictures.
- I will never meet in person an Internet "friend" without telling my parents and having someone I trust with me.
- It is my responsibility to browse safely. I will not look for inappropriate content, and I will tell my parents if I see something that upsets me.
- I will only download programs from the Internet that my parents have approved.
- I will not register to use Web sites or take surveys or quizzes that ask for personal information.
- I know that information posted on the Web can stay up there forever.
- I will think about with whom I am sharing information and be thoughtful about what is appropriate to share.

(Child's name) (Date)

（出典：http://www.atg.wa.gov/InternetSafety/FamiliesAndEducators.aspx）

2.4.　貯蓄上手なシニア　Savvy Saving Seniors

①目的・対象

高齢者と、高齢者へ財産管理のセミナーを提供する教育者のためのツールである。

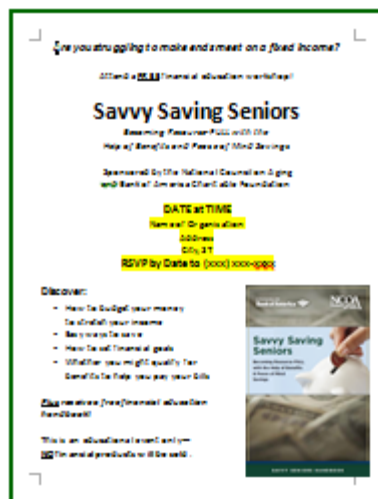
不利で弱い立場にある高齢者にとって、経済的な安定を保つには基本的な金銭管理が不可欠である。予算の立て方、詐欺の避け方、福祉手当の申請方法を学ぶことは、彼らの生活の安全を保ち、自立させる手助けとなる。全米高齢者問題協議会 National Council on Aging (NCOA) は、Bank of America Charitable Foundationよる支援を受け、高齢者に賢い財産・金銭管理スキルとヒントを伝授するセミナー「貯蓄上手なシニア」（Savvy Saving Seniors）の開催用に、財政教育ツールキットを開発した。これらを使用し、高齢者の世話に従事する職員らは、地域の高齢者に対しセミナーを提供する。2011 年に発行されたツールキットは、高齢者が詐欺のよくある手口を認識し、自身の財産を守るために適切な行動を取ることができるようになることを狙いとしている。その他、担当する教育者がワークショップを円滑に進めることができるための細かい助言も加えられいる。[10]

②提供方法

ツールキットはNCOA のウェブサイト[11]より無料でダウンロードすることができる。一部の資料は同サイトから印刷されたものをオーダーすることも可能だが、セミナーを開催する世話役向けのトレーニングガイドは一部＄10、参加者用のハンドブックは一部＄2 かかる。

ツールキットを用いた高齢者向けのセミナーは 90 分間を想定しており、参加費は無料で開催される。NCOA のウェブ上には、セミナーのマーケティング用の資料も揃っている(図 1.4.1)。

図 1.4.1：NCOAマーケティング資料

（出典：http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/savvy-seniors-marketing.html）

[10] http://www.marketwatch.com/story/new-tools-help-seniors-avoid-scams-2011-10-18 (12/01/2012)
[11] http://www.ncoa.org/calendar-of-events/how-to-facilitate-the-savvy-1.html (12/01/2012)

③様式・内容

セミナーの資料は 2 種類のツールキットで構成されている。ツールキット 1 は「助けになる－貯蓄マインドで福祉手当と安定を全面的に援助します（Becoming Resource-FULL with the Help of Benefits & Peace of Mind Savings）」、ツールキット 2 は「悪徳商法を避けるには（Avoiding scams）」というタイトルで、それぞれ以下の資料がネット上で公開されている。

－90 分のワークショップ用トレーニングガイド（PDF）
－プレゼンテーションスライド（PPT）
－参加者へのハンドブック（PDF）（全 28 ページ）
－参加者及び世話役の評価用紙（PDF）
－世話役のためのオンラインセミナー Webinar

ハンドブックの中には、参加者の財政感覚を把握するための 10 問のクイズ(図 1.4.2)、収支計画表（図 1.4.3）、一週間の実際の出費などが含まれている。クイズの内容は、回答者の支出行動や金銭管理について問うもので、5 択で回答する。全ての問題の後に、回答者の金銭感覚について簡単な診断結果を見ることができる。

隣のウェブページにある財政セキュリティ・リソースEconomic Security Resources サイト[12]も充実しており、13 種のオンラインセミナーが用意され、7 種のプレゼンテーション、ビデオ、出版物、レポートなど資料が揃っている。

図 1.4.2：参加者の財政感覚を把握するためのクイズと診断結果（ハンドブックより抜粋）

What's Your Money Personality Quiz

1. **When family/friends come to visit, I:**
   a. Order takeout.
   b. Buy frozen meals from the supermarket.
   c. See what I have in the fridge.
   d. Get out my recipe books.
   e. Ask my guests to bring something with them.

2. **How do you feel about money?**
   a. I don't think about it.
   b. I manage to get by somehow.
   c. I should think about it more.
   d. I keep pretty good control of it.
   e. I always end up with more than I started with.

3. **Saving money is:**
   a. Not something I'm interested in.
   b. Really hard to do.
   c. Something I aim for.
   d. Something everyone should do.
   e. The most important thing about money.

Mostly As—You're a debt collector's dream!

- You have very little awareness of your money and this could lead to trouble.
- If you continue like this, you risk getting into serious debt problems.
- It would be a good idea to learn more about controlling your money before it's too late.

Mostly Bs—You're a casual debtor.

- You like to live for the moment, and you don't think much further ahead than lunchtime.
- You usually don't know how much money you've spent or how much you've got left.
- If you're not careful, you could be an ideal candidate for debt.
- A little bit of planning can make your money work better for you and help you avoid stress.

Mostly Cs—You're a smart spender.

12 “Economic Security Resources” available at <http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/economic-security-resources.html> (13/12/2011)

図 1.4.3：収支計画表（ハンドブックより抜粋）

SAVVY SAVING SENIORS

Monthly Budget

My Income

Wages/Stipended Volunteerism	$________
Public Assistance	$________
Interest/Dividends	$________
Social Security	$________
Other	$________
Total Income	$________

My Expenses

Fixed Expenses

Rent/Mortgage	$________
Property Taxes/Insurance	$________
Car Payment	$________
Car Insurance	$________
Other Debt Payments	$________
Health Insurance	$________

13

SAVVY SAVING SENIORS

Flexible Expenses

Savings	$________
Gas/Oil	$________
Electricity	$________
Water	$________
Telephone/Cell Phone	$________
Food	$________
Transportation/Gas	$________
Car Maintenance	$________
Personal Expenses	$________
Charity/Donations	$________
Other	$________
Total Expenses	$________

14

世話役のためのオンラインセミナー Webinarはツールキットの使い方を詳しく説明しており、普及配布をより容易に行う際の助けとなる。

また、ツールキット以外にも、NCOAのウェブサイトには、高齢者がターゲットとなりがちな悪徳商法や詐欺のよくある 10 種の手口[13]、そうした被害から身を守るための 8 つの方法[14]など、経済的な安全を確保するための助言も掲載されている。

[13] http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/top-10-scams-targeting.html (12/01/2012)

[14] http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/top-8-ways-to-protect.html (12/01/2012)

3. イギリス

3.1. Protect My ID

①目的・対象

“Protect My ID” は、信用リスク管理や信用調査を手がけるグローバル企業、Experian 社が提供するサービスで、オンラインクレジット決済などに起因する個人情報漏洩、ならびにそれにより生じる詐欺被害を未然に防ぐことを目的としている。これは、クレジット記録のモニタリングや自分名義のクレジット決済が執行された際のアラート、また万一被害に遭ってしまった場合のアシストや保険を含む包括的なサービスで、利用料金は月額 6.99 ポンドである。[15]
広く一般市民を対象としている。

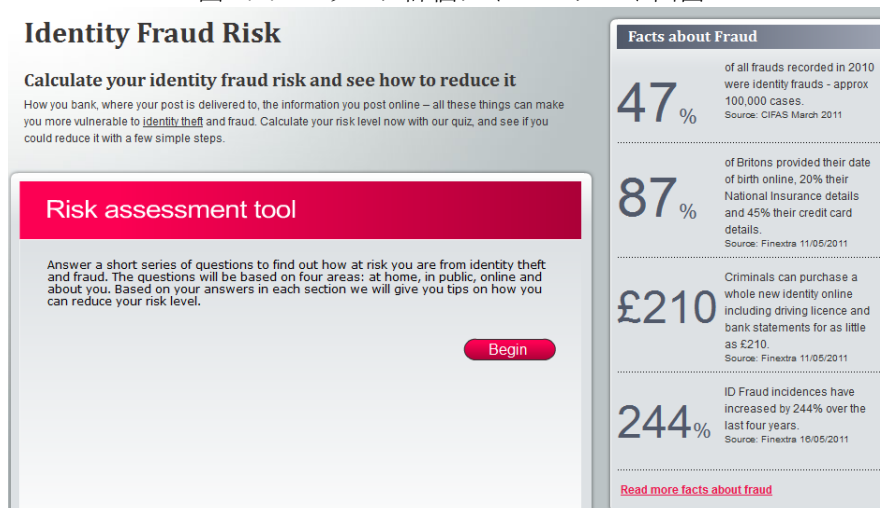
②提供方法

自身の日常的な行動パターンについての質問に答えることで、個人情報漏洩の危険性を判定し、リスクを回避するためのアドバイスを得ることができるリスク評価ツール[16]は、同社のウェブページ上で無料で利用することができる。

③様式・内容

リスク評価クイズのスタート画面左側には、個人情報を利用した不正行為、詐欺行為に関する事件・事故の情報が統計データを用いて解説されており、利用者への警戒を促している（図 2.1.1）。Read more facts about fraud をクリックすると、別のページで被害を防ぐために保守すべき個人情報が列挙されている。

図 2.1.2:　リスク評価クイズ スタート画面

(出典：http://www.protectmyid.co.uk/areyouatrisk.aspx?SiteVersionID=609&SiteID=100258&sc=501041&bcd=HM-NONE-PMID-ADBX-B1)

[15]http://www.protectmyid.co.uk/WhatYouGet.aspx?link=bottommodule&SiteVersionID=609&SiteID=100258&sc=501041&bcd=HM-NONE-PMID-ADBX-B1 (19/12/2011)
[16]http://www.protectmyid.co.uk/areyouatrisk.aspx?SiteVersionID=609&SiteID=100258&sc=501268&bcd=ActionFraudresources&areaid=0&pkgid=UKPNO (19/12/2011)

質問は以下の 5 項目に分かれている。

- 家庭生活環境 (At Home)
- 家庭外での日常的な行動 (In Public)
- オンラインでの活動状況 (Online)
- 携帯電話の利用状況 (Mobile)
- その他個人の行動パターン (About You)

図 2.1.3: リスク評価クイズの質問ページ

(出典：同上)

それぞれの項目で 4〜5 問ずつ、上記の順番で出題され、各項目で全て回答しないと次に進むことができない。回答は全て選択式で、Yes または No による回答のほか、質問によっては該当する行動を取る頻度や携帯しているクレジットカードの枚数などを選択し回答するものもある。

質問内容は、「ダイレクトメールをシュレッダーにかけるか」、「オンラインショッピング・バンキングを利用しているか」、「ウィルス対策ソフトを更新しているか」といった、情報セキュリティの保守に直接的に影響することが明白なものに加え「レストランで頻繁に外食をするか」、「運転免許証を携帯しているか」、「Facebook や Twitter などの SNS を利用しているか」、「携帯電話からインターネットを利用するか」といった、多くの人の日常的な行動に該当すると考えられるものも含まれている。

全ての質問を終了すると、回答に応じ High、Medium（うち Medium-High、Medium、Medium-Low）、Low の 5 段階でリスクレベルが判定される。さらに、個別の回答に基づき具体的なアドバイスが提供される。結果は印刷することも可能である。

同社ウェブサイトには、個人情報を利用した詐欺事件や被害者に関する情報をまとめたブログも掲載されている。[17]また、詐欺被害の実例が 5 つ紹介されている。[18]また、同社はTwitterなどSNSを利用し、広く一般に向け安全喚起を行っている（@Protect My ID）。

同リスク評価ツールは、詐欺被害を専門で取り扱う英国の公的機関Action Fraudのウェブページにも、Risk Assessment Quizとしてリンクが掲載されている。[19]Action Fraud は、英国の犯罪をつかさどる行政機関Home Office やロンドン市警などと提携し、詐欺行為予防のための情報提供や被害者のサポートを手がけている。[20]同機関のウェブページにおいても、詐欺被害に関する実例や、被害を未然に防ぐためのアドバイスが閲覧可能なほか、万一被害に遭ってしまった場合に力になってくれる有益なコンタクト先の情報を得ることができる。

---

[17] http://blog.protectmyid.co.uk/
[18]http://www.protectmyid.co.uk/HowIdentityProtectionWorks.aspx?link=bottommodule&SiteVersionID=609&SiteID=100258&sc=501003&bcd= (15/12/2011)
[19] http://www.actionfraud.org.uk/resources (15/12/2011)
[20] http://www.actionfraud.org.uk/about-us (15/12/2011)

3.2. Personal Security Checklist

①目的・対象

個人情報の保護や、コンピューターの安全性を保つために必要な行動を促す。また、関連するリスクを軽減するために知っておくべき情報の普及を目的とする。
対象は一般および経営者で、個人用[21]とビジネス用[22]の質問が用意されている。

②提供方法

Get Safe Online のウェブサイトで公開されている。メインページにある内容は、ウィンドウズ OS 利用者を想定したものであり、Mac および Linux ユーザー向けの情報は別のページに用意され、それぞれリンクが貼られている。

③様式・内容

ソフトウェアの有無や電子メールの利用状況に関する質問(10 問)に回答する。質問は YES/NO の 2 択式がほとんどである（図 2.2.1）。全て回答すると、回答に応じた詳細なアドバイスを得られ、これが利用者ごとにカスタマイズされたチェックリストの役割を果たす。希望者には、結果を電子メールで送信してくれる。

図 2.2.1：ソフトウェアの有無や電子メールの利用状況に関する質問のページ

[21] http://www.getsafeonline.org/nqcontent.cfm?a_id=1111 (15/12/2011)
[22] http://www.getsafeonline.org/nqcontent.cfm?a_id=1275 (15/12/2011)

質問項目は以下の通りである。

- アンチウィルスソフトウェア
- ファイアウォール
- アップデート
- スパイウェア
- バックアップ
- 迷惑メール
- ワイヤレスネットワーク
- ブラウザ
- 電子メール
- その他（ウェブツールなどの利用）

アドバイスのページでは、トピックに関する基本用語や専門用語には用語集（Glossary）へのリンクが付けられており、利用者の理解を助ける工夫がされている（図 2.2.2）。

図 2.2.2：アドバイスのページ

Secure wireless networks

Without protection, Wi-Fi (wireless) networks are vulnerable

Wi-Fi (wireless) networks are vulnerable to eavesdropping, hackers and freeloaders.

Why protect wireless networks?

Wireless networks, which are sometimes known as Wi-Fi or 802.11 networks, let computers talk to one another using a radio link similar to cordless phones.

Like any radio transmission, anyone in range can pick up the signal or transmit on the same frequency. This means that wireless networks are at risk from:

- Eavesdropping – listening to the information as it is transmitted over the air. This means that information on the network must be encrypted
- Hacking – anyone in range can connect to the network. This means that the network must be restricted to known and trusted users and computers.
- Freeloading – where a wireless network is used to share a broadband internet connection, there is a risk that unauthorised users will use your connection without permission.

The problem is that most wireless network equipment, when it comes out of the box, is not protected agains these threats in order to make it easy to set up. This means you have to configure the network yourself to make it secure.

How to protect a wireless network

Although the Wi-Fi standard defines things like encryption and access control, the way you set them up varies from manufacturer to manufacturer. This means that the advice will seem a little technical because it is only possible to say what you have to do, not how you do it. Consequently, you will need to refer to the documentation that came with your hardware to set these defences up.

- Use encryption. WPA or WPA2 are the best. Failing either of these, for example if you are using older access points and network cards, use WEP.
- Use a strong password on the wireless access point to control administrator access (see Use strong passwords).

その他、同ウェブサイトには、コンピューターがウィルスに感染してしまった場合のサポート情報や、親・教員・子供たち向けのオンラインでの安全性に関するアドバイス、個人情報保護、手持ちの PC をハッキングなどのリスクから守るための情報が掲載されている。

また、ツイッター(@GetSafeOnline) やFacebook（https://www.facebook.com/GetSafeOnline）、ブログ[23]などを使い、オンラインでの安全性に関するニュースや情報の普及を行っている。

[23] http://feeds2.feedburner.com/GetSafeOnlineBlog (15/12/2011)

3.3. インターネットを活用する（'Making the most of the internet'）インターネット安全性（Internet security: Staying safe online）

①目的・対象

Age UK グループは、Age Concern England と Help the Aged による 2009 年 4 月の設立以来、高齢者の生活の充実を促進するサービスやサポートを提供している。具体的には、高齢者に対し、フリーダイヤルによる情報やアドバイス提供、高齢者が直面する問題に関する意識の向上、政策改善のキャンペーン、また高齢者の自立を促すサービスや製品の紹介やトレーニングを提供している。

こうしたサービスの一環として、高齢者に対しコンピューターやインターネットの使い方を普及させると共に、インターネット上での情報セキュリティに関する注意喚起を促し、安全性を保つためのチェックリストを提供している。

②提供方法

Age UK が発刊する、高齢者向けのインターネット利活用を促す資料に、「インターネットを活用する」（'Making the most of the internet'）[24]と「インターネットの安全性」（'Internet security: Staying safe online'）[25]がある。いずれの資料もAge UKのウェブページからダウンロードすることができる。この他、希望者には無料で紙ベースの冊子の送付を行い、ニーズに応じ通常版よりも文字が大きく印刷された資料の準備もある。また、オーディオでの情報提供も行っている。

Action UK ではこの他、高齢者向け IT トレーニングを専門とする Digital Inclusion Network と提携し、英国各地でコンピューター利用のトレーニングを開催するなど、高齢者の情報技術利用に関する自己啓発を促している。

③様式・内容

(1)「インターネットを活用する」（'Making the most of the internet'）

同冊子は、コンピューターを初めて利用する高齢者にわかりやすく基本的な用語を解説しているほか、インターネットが生活にもたらす利便性を、電子メールや検索機能などの活用方法と共に紹介している。各機能の具体的な使い方ではなく、それぞれを使ってどんなことができるかといった基本的な情報に焦点が置かれている。

以下に、主な内容を紹介する。

Getting Started および Getting Online：デスクトップ・ラップトップコンピューターの紹介に始まり、インターネットへの接続方法、キーボードやマウスなど必要なツールがわかりやすくまとめられている。

---

[24] http://www.ageuk.org.uk/Documents/EN-GB/Information-guides/AgeUKIG22_Making_the_most_of_the_internet_inf.pdf?dtrk=true (19/12/2011)
[25] http://www.ageuk.org.uk/Documents/EN-GB/Information-guides/AgeUKIL4_Internet_security_inf.pdf?dtrk=true (19/12/2011)

Keeping in touch: 電子メール、インターネット電話、ソーシャルネットワーキングサイト（SNS）の機能の紹介と、SNS や出会い系サイトを利用する際の個人情報保護の注意喚起。
Saving time and money: オンラインでのショッピング、行政サービス、旅行手配などの紹介。
Information and advice: 情報検索の基本的な方法。特に税金や給付金、健康に関する情報検索に有益なウェブページを紹介している。
Staying active: 趣味やテレビ・音楽を楽しんだり、ニュースの閲覧、就職活動やトレーニングコースの検索に役立つウェブサイトを紹介している。
Useful organisations: Age UK やアルツハイマー協会など、高齢者のサポートを行う組織の他、オンラインの安全性を促進する組織、コンピューターやインターネットの利用を支援する総合サポート団体、消費者保護団体などの連絡先やウェブサイトが掲載されている。
Glossary: コンピューターやインターネットに関する基本用語を解説している（図 2.3.1）。

図 2.3.1：基本用語解説の抜粋

Glossary

Bandwidth
A measure of how much information can be transferred within a given amount of time in megabits per second, or 'Mbps'.

Dongle
A small device you can plug into your laptop to access broadband internet on the move.

Download(ing)
Transfer files from the internet to your own computer. When used with email, it usually refers to collecting new messages. When used with the web, it usually refers to requesting a web page.

Email(ing)
Short for 'electronic mail'. Email is the internet version of the postal service: you send a message (also referred to as 'emailing') from your computer to another person who also has access to email.

Hard drive
The disk inside your computer where your documents, photos and software are stored.

Internet/the net
A worldwide collection of computers joined by networks, which are linked to each other via communication links such as telephone lines. To join the internet all you have to do is connect your computer to one of the networks.

また、ところどころにインターネット利用経験のある高齢者の体験談に見立てたエピソードを盛り込み、読者の動機付けを行っている（図 2.3.2）。

図 2.3.2: インターネット利用者の体験談（'Making the most of the internet'より抜粋）

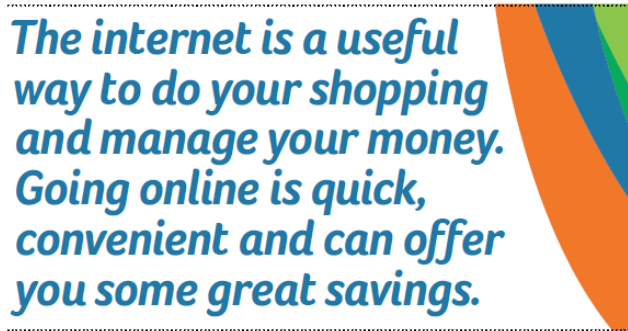
'I was secretly heartbroken when my eldest daughter accepted a job in America. I thought I'd lose all contact. But now I have learned to use email, it has helped us to keep in touch and I also managed to book my flights online to visit her. I couldn't believe how simple it was.'
Margaret, 58

(2)「インターネットの安全性」（‘Internet security: Staying safe online’）

同冊子は、インターネット上での個人情報の保護やコンピューターの保護について解説している。導入部分では「（インターネットに明るくなくても）長い人生で培ってきた判断能力や飛び込み営業の電話を交わす方法などをインターネットに適用すれば、オンラインでも自身の身を守ることができるので心配無用」という旨を謳っている。[26]

以下に、主な内容を紹介する。

Email encounters: フィッシングの手口と見分け方、迷惑メールの対処法など。
Telephone scams: 個人情報取得を目的とした電話による詐欺への注意喚起。
Online shopping and banking: オンラインショッピングとバンキング利用時の注意点を列挙。
Social networking: ソーシャルネットワーキングサイト利用時の注意点。
Protect your computer: 手持ちのコンピューターを安全な環境に保つためのチェック（’SAFE’）を紹介している。[27]

S=Spy-ware をインストールする。
A=Anti-virusソフトをインストールする。
F=Firewallを有効にする。
E=オペレーティングシステムがアップデートされていることをEnsure（確認）する。

Useful organisations: コンピューターやインターネットの利用に関する見識を深めるために有益な団体の連絡先やウェブサイトを紹介している。
Glossary: アンチウィルス、ファイアウォール、フィッシングなど、安全性に特化した用語の解説をしている。

題目の通り、インターネット上に潜む危険と、被害を未然に防ぐための対策や情報などから構成されているが、インターネットが生活にもたらす利便性が簡潔にまとめられた文章が、全編を通じ随所に挿入されている（図 2.3.3）。危険を強調するあまり、高齢者をインターネットの利用から遠ざけないための工夫ともうかがえる。

図 2.3.3：インターネットの利便性を強調する記述（「インターネットの安全性」（‘Internet security: Staying safe online’）より抜粋）

いずれの資料も、大きなフォントで簡潔でわかりやすい文章で書かれ、高齢者にとって読みやすいよう配慮がされている。さらに、キーワードは太字表記され解説が加えられ、巻末には便利な連絡先や関連用語集が設けられ、理解が深められるよう配慮がされている。

[26] http://www.ageuk.org.uk/Documents/EN-GB/Information-guides/AgeUKIL4_Internet_security_inf.pdf?dtrk=true (p.2) (19/12/2011)
[27] Ibid. (pp. 12-13) (19/12/2011)

4. ドイツ

4.1. ドイツ連邦情報セキュリティ局ITセキュリティガイドラインBSI: Leitfaden IT-Sicherheit

①目的・対象

主に中小企業のITマネージャーや管理部門の職員を対象としている。[28]

ドイツでは、連邦情報セキュリティ局 (Bundesamt für Sicherheit in der Informationstechnik: BSI)の定めるITベースライン保護（IT-Grundschutz）が、ITセキュリティの最も包括的な基本方針として、多くの企業や公的機関に採用されてきたが、IT技術の進歩とともにIT-Grundschtzの内容も複雑化してきた。中小企業においては財政的資源および人的資源に限界があり、IT の専門知識を有する職員がいない場合もある。そのような状況下でも、誰でも簡単にITセキュリティの導入をすばやく実行できることを目的とし、従来のIT-Grundschetzに代わり、最も重要な項目を簡潔にまとめたサポート資料、ITセキュリティガイドライン（Leitfaden IT-Sicherheit）が2006年に発行された。同冊子には、ITセキュリティの最も重要なセーフガードの簡潔な概要がまとめられている。

②提供方法

ネット公開型PDFをダウンロードする提供方式。第5回IT基準プロテクションデー（IT-Grundschutz-Tag）が2011年11月30日にボンで開催されており、当ガイドラインを含むITセキュリティ関連の冊子が配布された可能性が高い。多言語対応で、ドイツ語版、英語版、エストニア語版を用意している。[29]

③様式･内容

ITセキュリティガイドラインドイツ語版PDF（全87頁、2006年）：
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

英語版(英語版は簡易版のみ)PDF (全49頁、2007年6月):
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf?__blob=publicationFile

同冊子では、まずITセキュリティに関する重要なコンセプト、国内での法的な規制が説明されている。さらに、適切な準備を怠ったために招いたデータの損失やウィルスの観戦の事例をケーススタディ仕立てで5例紹介し、そのような事態に陥らないために取るべき手段を紹介している。また、ITセキュリティ保持を行う上で頻繁に見られる間違い（人的ミス）として7例を紹介し、注意を喚起している。

---

[28] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf?__blob=publicationFile (p.3) (07/01/2012)

[29] https://www.bsi.bund.de/ContentBSI/grundschutz/intl/intl.html (07/01/2012)
https://www.bsi.bund.de/ContentBSI/EN/Topics/ITGrundschutz/ITSecurityGuidelines/guidelines.html (07/01/2012)

基礎的な最低限のセキュリティセーフガードとして、50 項目が挙げられており、それぞれに補足／解説が付けられている。[30]

企業の IT 部門や管理部門を対象としているため、終始事務的な内容で、図や写真の挿入もなく、用語の解説等も付いていない。しかし、IT セキュリティの専門知識をもたない担当者であっても内容を容易に理解できるよう、実際に起こりうる状況のケーススタディを用いた説明や、ポイントと解説を併記した記述などの工夫が施されている。

巻末のチェックリスト(ドイツ語版 pp.74-79; 英語版 pp.42-45)は、情報セキュリティ対策を約 50 項目に要約し、企業または団体の弱点を簡潔かつすばやく俯瞰できるよう作られている（図 3.1.1）。

図 3.1.1: IT セキュリティガイドラインのチェックリスト(英語版)

IT security management	
❐	Has management defined the IT security objectives and accepted that they are responsible for IT security? Have all the legal and contractual issues been considered?
❐	Is there an IT Security Officer?
❐	Are IT security requirements considered early on in every project (e.g. during planning of a new network, new purchases of IT systems and applications, outsourcing and service agreements)?
❐	Is there a summary of the most important applications and IT systems and their protection requirements?
❐	Is there an action plan that prioritises security objectives and defines how the agreed IT security safeguards should be implemented?
❐	Has it been determined for all IT security safeguards whether they have to be carried out once only or at regular intervals (e.g. updates to the anti-virus software)?
❐	Have responsibilities been defined for all the IT security safeguards?
❐	Are appropriate deputisation arrangements in place for persons in positions of responsibility and are the stand-ins familiar with the tasks they have to perform in this capacity? Have the most important passwords been securely deposited for emergencies?
❐	Are all involved persons familiar with the existing policies and responsibilities?
❐	Are there checklists covering factors that need to be considered when new staff join or existing staff leave the company (authorisations, keys, training etc.)?
❐	Is the effectiveness of IT security safeguards checked regularly?
❐	Is there a documented IT security concept?

チェックリストは以下の各項目（それぞれ 3ー12 問）により構成されている。

- IT セキュリティのマネジメント：組織に IT セキュリティを保守する体制があるか？
- IT システムの安全性：ウィルスソフトの有無やシステムの管理体制
- ネットワークとインターネット接続: ファイアウォール、コンフィギュレーションに関して、トレーニング状況など
- コンプライアンス：機密情報の取り扱いについてなど
- IT システムのメンテナンス状況
- パスワードと暗号化
- 継続性の計画（不測の事態のバックアップの準備状況）
- データバックアップ
- インフラの安全性

「ITベースライン保護プロフィール」(“IT-Grundschutz-Profile”)は、ITセキュリティガイドラインにて定められる 50 の最も重要な情報セキュリティ基準を遵守すべく、企業内にて体系的

[30]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf?__blob=publicationFile pp.17-35 (07/01/2012)

にITセキュリティ概念を構築する手引き書の役割を果たしている。[31]組織の規模に応じ、小企業(2008 年)、中小企業(2010 年)、大企業(2004 年 11 月)、産業(2008 年)向けの 4 種が用意されており、殊に小企業向けの資料には、上記のセキュリティガイドラインとは別種の 63 項目のチェックリストが含まれている(ドイツ語版pp.51-56; 英語版 pp.49-53)(図 3.1.2)。同チェックリストは、企業や組織におけるITセキュリティ保守の手順や対策を文書化するための助けとなる。

図 3.1.2：小企業向け IT ベースライン保護法プロフィールのチェックリスト（英語版）

11.6 Checklist

No.	Question
Q1. ☐ ☐	Have the following issues been defined in your IT security policy? - Importance of IT security and relevance of the IT to your company - Definition of IT security objectives
Q2 ☐	Have your employees been made sufficiently aware as regards IT security?
Q3 ☐	In the past 12 months have you updated the security policy, the protection requirement assessment and the PC passports or are you just about to do it?
Q4 ☐	In the PC passport have you already entered the contact and the hotline telephone numbers for all IT systems?
Q5 ☐	Do you have a specific contact to turn to when problems occur with the computers, programs/applications, and have you entered his/her telephone number (hotline telephone number) in the PC passport?
Q6 ☐ ☐ ☐ ☐	Have you informed your employees that a password - needs to be changed on a regular basis, - must include at least 8 characters, - should not be easy to guess (like husband's first name, own car ID etc.) and - must be recorded and stored in a closed envelope?
Q7 ☐	Do you have a shredder in your organisation?

小企業向けITベースライン・プロテクションプロフィールのドイツ語版PDF (全 70 頁、2008 年): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/it-grundschutz_profil_klein.pdf?__blob=publicationFile

英語版は小企業向けのみ 。PDF (全 66 頁、出版年不明):
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_small_organisation_pdf.pdf?__blob=publicationFile
このほか、BSIは、組織においてIT-Grundschutzの基準を満たすITセキュリティの基本理念を構築、管理、更新を支援する支援するためのソフトウェアツールIT-Grundschutz tool (GSTOOL)を開発、提供している。[32]

[31]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_small_organisation_pdf.pdf?__blob=publicationFile p.1 (07/01/2012)
[32]https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzGSTOOL/itgrundschutzgstool_node.html (07/01/2012)

4.2.　ネットでの安全 - IT セキュリティ CD (Sicher ins NetzDie IT-Sicherheits CD)

①目的・対象

ヘッセン州とドイツテレコムが共同開発した CD で、家庭、ビジネス、公共機関における IT システムの安全な使い方、特にインターネット上における危険や脅威から、コンピューターとデータを守るという点に焦点を置き、教育促進することを目的としている。IT の専門用語に詳しくない人でも学習できるように作成されている。Ver.1 は 2005 年、Ver.2 は 2007 年にスタートした。

IT 初心者からプロフェッショナルまでを対象とした全てのコンピューターユーザー（IT 初心者、ホームユーザー、学生、中小企業）の IT セキュリティに関する自習用のマルチメディア教科書という位置づけで提供されている。

②提供方法

下記のウェブサイトから無料でダウンロード、または CD をメールオーダーすることも可能。ウェブ上で体験することもできる。ただし、言語はドイツ語のみである。
http://www.hessen-it.de/sicherheit/Inhalte/Branding.html

配布に当たっては、TVやメディアなど広範なマスコミ報道が行われた。CDは無料であるため、ヘッセン州外へも普及し、ドイツテレコム側も顧客や社員にも配付し普及に努めた。2005 年 7 月以降、2 万部のCDが配布されたが、高まる需要を満たすべく、2007 年末までに 1 万部のCDが配付された。[33]

③様式・内容

冒頭では、電子メールのウィルスで会社全体のシステムが麻痺してしまった、コンピューターがクラッシュしたなど、日々メディアで報道される IT 関連の事故を例に挙げ、セキュリティの大切さを訴えている。

CD は利用者の IT セキュリティに関する知識レベルを明らかにするコンピタンス（能力）チェックから始まる。一般的なインターネット、コミュニケーション技術、脅威に関する問題 8 問に対し、程度に応じ 4 択で回答する。脅威を防ぐためのアドバイスと対策などが紹介されている。

コンピタンスチェック項目

(1) インターネットの基本的サービス（電子メール、WWW など）の機能を知っている。
(2) インターネットユーザー間のコミュニケーションのプロセスを説明できる。
(3) モデムとルーターの役割と機能を知っている。

[33] ENISA (European Network and Information), *Information security awareness: Local government and internet providers*, August 2007
http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Information%20Security%20Awareness%20Initiatives%20Undertaken%20by%20Local%20Governments%20and%20ISPs%20in%20the%20EU_FINAL.pdf pp.46-47 (07/01/2012)

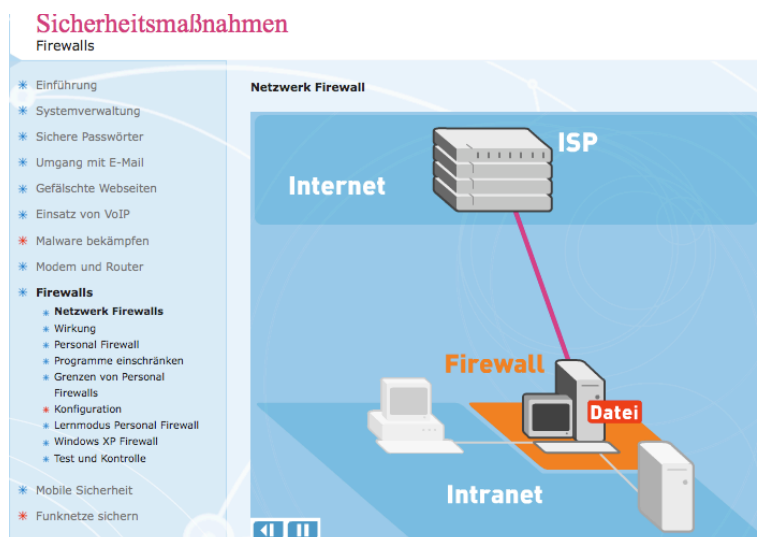
(4) プロトコル、ルーター、バックボーンなど専門用語を説明できる。
(5) インターネット上での攻撃（脅威）について認識している。
(6) ウィルスやトロイの木馬など、悪質なプログラム各種を知っている。
(7) ウィルスや悪質プログラムに感染した場合がわかる。
(8) 上記にのような攻撃に対する対策を知っている。

図 3.2.1：コンピタンスチェックのページ

Gefahren und Angriffe（脅威と攻撃）のページでは、フィッシングやファーミングの解説、ネットワークの脅威や悪質プログラムの種類別に細かく説明が加えられている（図 3.2.2）。

図 3.2.2：危険と脅威のページ

Sicherheitsmaßnahmen（安全対策）ではパスワード管理の方法、偽ウェブサイトを見分けるチェックリスト、ファイアウォールの仕組みなどが解説されている。イラストや写真はなく、文章による説明が多いが、一部動画と音声による解説も入る（図 3.2.3）。

図 3.2.3：ファイアウォールの説明のページ（動画アニメーション）

利用者は以下のカテゴリーで自習を進めることができる。

(1) ベーシックツアー: インターネットとセキュリティの基本事項。
(2) インターネット基礎：インターネットの基本的な操作方法。
(3) 脅威と攻撃：インターネットに潜む危険性と、手口の説明。
(4) セキュリティ対策：リスクを軽減し、守備を固めるための情報、指示、ヒント。
(5) 理解度確認クイズ

説明トピックにはウィルス、ウォーム、スパム、トロイの木馬、ダイヤラー、スパイウェア、Eメール盗聴、ポートスキャニング、スニフィング(ネットワーク上を流れるデータを傍受すること)、インターネットバンキング、オンラインショッピング、オンラインオークション、暗号化、ウィルス防御プログラム、ファイアウォール、フィッシング詐欺、ファーミング詐欺(事前に偽サイトを作り、ユーザーに気づかれることなく偽サイトに誘導して収穫を得ること)、ボットネット(悪意のある攻撃者が構築するネットワークで、命令によって遠隔操作されるコンピューター群のこと)、ヴォイスオーバーIP (IP電話のようにIPネットワーク上で音声通話を行う技術)、移動通信セキュリティ、パスワードセキュリティなどが含まれる。[34]

[34] http://www.hessen-it.de/dynasite.cfm?dsmid=13688&num=11705 (07/01/2012)

4.3. 「50 歳以上をネットワークへ」“50+ ans Netz” - Online-Jahr 50plus 2006-2007

①目的・対象

2006 年から 2007 年にかけて実施された、ドイツの 50 歳以上の市民を対象とする取り組みである。
ドイツにおける高齢者のインターネットの利用は 2000 年台後半以降急速に高まっているが、未だ 40%程度に留まっており、欧州の平均値と比較しても低迷している。[35]このためドイツでは、インターネットに触れた事がない世代、特に高齢者を対象に、インターネットの利用を推進するための取り組みが積極的に導入されている。ドイツテレコム社、ドイツ連邦高齢者協会（Die Bundesarbeitsgemeinschaft der Senioren-Organisationen: BAGSO）とコンピーテンスセンター(Kompetenzzentrum Technik-Diversity-Chancengleichheit e.V.)は、2006 年 5 月から 2007 年 7 月にかけて、“50+ ans Netz”（「50 歳以上をネットワークへ」）という取り組みを実施、インターネットコースやコンペなどの数々のイベントを高齢者を対象に開催した。同事業は、その後ドイツ国内各地で展開されてきた同様の取り組みの礎を築いている。

“50+ ans Netz” は、コンピューターやインターネットを使った経験のない 50 歳以上の市民を対象に、以下を狙いとして実施された。
- インターネットの利用がもらす利便性と機会を紹介し、興味を促す。
- コンピューターやインターネットに関する一般的な知識を提供する。
- 利用者の興味にあった内容のコースを安全かつ安価にて提供する。
- グループによる学習。

②提供方法

実際に参加者がコンピューターに触れる講義形式の講習、ワークショップ、イベントなどが、全国 297 の市町村で実施された。[36]宣伝のために、66 万枚のフライヤーとポスター[37]が用意、配布された。また、連邦政府家庭・高齢者・女性・青少年省（Bundesministerium für Familie, Senioren, Frauen und Jugend）発行の高齢者のための情報冊子 「年齢は新しいものを創り出す- 高齢者のための取り組みと情報（“Alter schafft Neues - Initiativen und Informationen fur altere Menschen”）」 にも、インターネット利用促進のための有益な取り組みとして紹介されている。[38]

BAGSOは、「高齢者のためのインターネット世界へのガイド（"Wegweiser durch die digitale Welt - Für ältere Bügerinnen und Bürger"）」 をはじめ、インターネットや電子メールをはじめ、新たなコミュニケーションチャネルの利用を高齢者に促進するための無料の資料やガイドの配布を行っている。[39]これらの資料はBAGSOのウェブサイトからダウンロード可能なほか、BAGSOのメンバー組織の開催する高齢者向けのイベントでも配布されている。[40]

---

[35] der Bundesregierung auf die Kleine Anfrage der Abgeordneten Britta Haßelmann, Grietje Staffelt, Ekin Deligöz, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 16/10379 –
http://dipbt.bundestag.de/dip21/btd/16/105/1610540.pdf (16/01/2012)
[36] http://www.internetpaten.info/Digitale-Integration/Aeltere-Erwachsene/Online-Jahr (07/01/2012)
[37] Ibid.
[38] http://www.bmfsfj.de/RedaktionBMFSFJ/Broschuerenstelle/Pdf-Anlagen/Alter-schafft-Neues,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf pp.65-66 (07/01/2012)
[39] http://www.bagso.de/publikationen.html よりダウンロード可能。
[40] ドイツ連邦共和国家庭・高齢者・女性・青少年省にメールで確認した（13/01/2012）。

③様式・内容

インターネット利用に関する講習の内容は、日常的に頻繁に直面する以下の 5 つのトピックに絞られ、実用的な構成となっている。いずれもコンピューター初心者で、スキルのない人を対象としており、興味のあるモジュールを選択し参加する。各モジュールの策定に協力したパートナーを括弧内に記す。

- ショッピング：オンラインストア、商品選ぶ、決済。（T-Online）
- ファイナンス：オンラインで口座チェック、送金など（ドイツ郵便貯金）
- 健康：健康に関する情報やガイド、栄養やケアに関する情報の検索（BKK24）
- トラベル: オンラインでの旅行計画、チケット予約方法、発券の方法など（ドイツ国鉄）
- セキュリティ：ジャンクメールの対処方法、ウィルスや不正アクセスからどうコンピューターを守るか。(シマンテック)

コースはいずれも 4 時間で、前半はマウスの使い方、インターネットサーフィン・電子メール、オンラインでの情報検索方法、インターネットのインタラクティブな利用方法などについて、基本的な内容を押さえ、後半はそれぞれのトピックを深堀りする構成となっている。

各コースへの参加費用は 20 ユーロで、年齢に応じて 10 セントずつの割引が適用され、年齢が高いほど割安となる。

コースの教材は 16 万部用意された。[41]インターネットの概要に加え、電子メールの書き方／送り方、サーチエンジンを使った情報検索の方法を中心に、図を用いて順を追って説明されている。[42]（図 3.3.1）

図 3.3.1: コース教材より抜粋（情報検索方法の解説）

“50+ ans Netz”では講習の他にも、コースへの最年長参加者への表彰を行うなど、参加者の意欲を高めるようなイベントを開催した。また、作文コンテストを実施し、『インターネットの良い点？困った点？”Was begeistert Sie am Internet? Was ärgert Sie?”』というテーマで応募を募った。これは、主催者である BAGSO にとっても良いフィードバックとなった。

[41] http://www.internetpaten.info/Digitale-Integration/Aeltere-Erwachsene/Online-Jahr　07/01/2012）
[42] Kompetenzzentrum (2006) “Online-Jahr 50plus Internet verbindet“

2006 年 9 月には、オンラインアクションウィーク”Aktionswoche Online-Jahr 50plus - Internet verbindet”が設けられ、情報提供イベントや、参加者が出題された問題の答えをインターネットで検索し回答するインターネットクイズなど、参加型のゲームやアクティビティが行われ、習得したスキルを披露する機会が提供された。

連邦政府経済テクノロジー省により 2008 年から実施されている取り組み”Internet erfahren” (インターネット体験) の主要プログラムの一つに、BAGSOの “erlebnis internet erfahrung schaffen”（インターネット体験の創出）が名を連ねている。[43]これは、”50+ ans Netz” 同様、インターネット初心者に最初のきっかけを与える事を目的としているが、インターネットを利用するための講習会を実施するのではない。代わりに、高齢者が多く所属するスポーツクラブなどで、『インターネットを使えば自宅でエクササイズを作れますよ』、『ヘルシーで栄養のあるレシピが紹介されていますよ』と、インターネット以外の興味とセットにしてインターネットの利便性や使い方を紹介することで、利用のきっかけを促す。同年代の仲間がいる慣れ親しんだ環境できっかけを植え付けることで、自分は高齢だから、または知識がないから怖いなどの理由でインターネットの利用に踏み切らない高齢者の背中を押している。[44]

インターネットを利用していない（できない）人口を半減させようというEUレベルでの取り組みの下、ドイツでは、インターネットをはじめとするデジタルツールの国民全体（高齢者、障害者、学習障害を持つ者を含む）への広い普及を目指し、政府主導の様々な事業が展開されている。[45]

[43] http://www.bmwi.de/BMWi/Navigation/Technologie-und-Innovation/Digitale-Welt/Digitale-Gesellschaft/internet-erfahren,did=299118.html （07/01/2012）

[44] Bundesministerium für Wirtschaft und Technologie (BMWi) (2011) “Erlebnis Internet – Erfahrung schaffen” p.44

[45] http://www.internetpaten.info/Digitale-Integration/Aeltere-Erwachsene （07/01/2012）

4.4. 「誰だか当ててみて－詐欺師と泥棒の手口から身を守るには」"Rate mal, wer dran ist? So schützen Sie sich vor Betrügern Trickdieben"

①目的・対象

「誰だか当ててみて－詐欺師と泥棒の手口から身を守るには（Rate mal, wer dran ist? So schützen Sie sich vor Betrügern Trickdieben）」は、ドイツ連邦共和国家庭・高齢者・女性・青少年省（Bundesministeriums für Familie, Senioren, Frauen und Jugend）により 2011 年 3 月 25 日に出版された、高齢者向けの情報提供資料である。高齢者は多額の資産や財産を有し、日中を自宅で過ごすことが多く、また独居であることも多いため、日々犯罪のターゲットとして危険に晒されている。高齢者が犯罪の典型的な詐欺行為に気が付き、被害を未然に防ぐこと、また万一被害に遭ってしまった場合に迅速に対処できるようになることを目的としている。

②提供方法

PDF資料を連邦共和国家庭・高齢者・女性・青少年省のウェブサイト[46]から無料でダウンロードすることができる。同じサイトで、希望者は一団体 5 部まで印刷された冊子をオーダーすることも可能。6 部以上必要な場合はメールで注文する。また、紙ベースの冊子は、自治体の高齢者課や同省の主催するイベント（ドイツシニア市民デー: Deutscher Seniorentagなど）でも配布されている。[47]いずれの場合も無料である。

③様式・内容

全 60 ページからなる同冊子は、以下の 9 章より構成されている。最初の 2 章で同冊子の狙いと高齢者がターゲットになりやすい詐欺、窃盗などの概略を簡単に説明した後、具体的な対策や対処法が紹介されている。

1. 高齢者と犯罪脅威
2. 虚偽、トリック、犯罪者の高齢者戦略
3. なぜ高齢者は潜在的犯罪者の詐欺対象として興味を引くのか？
   高齢者は往々にして多額の財産を有している、また日中自宅にいることが多く、特に女性は独居が多い。警察への通報率も低い（犯罪に遭ったという汚点を残したくない、家族に迷惑をかけたくないなどの理由もある）、犯罪者を覚えていないので、万一通報されても逃れられることが多い。
4. 犯罪はどのように起こるのか？
   犯罪者は往々にして過去に接触し面識がある人や過去に助けてくれた人であることが多い、と注意を喚起。よくある手口として、日本の「オレオレ詐欺」に類似した、親戚（甥や姪）を装って電話をかけ、金銭を要求するケースや、配水管工事などを装い自宅へ潜入し犯行に及ぶ例などが挙げられている。また、高齢者のインターネット利用度の増加に伴い多発が予想されるオンライン取引詐欺の例も指摘している。また、物理的な窃盗や振込み詐欺行為の他、悪徳商法の事例も紹介している。このように、代表的な犯罪の手口を約 20 ページに渡り紹介している。
5. どのようにして犯罪者を見分けられるのか？

---

[46] http://www.bmfsfj.de/bmfsfj/generator/BMFSFJ/Service/Publikationen/publikationen,did=126226.html（07/01/2012）

[47] ドイツ連邦共和国家庭・高齢者・女性・青少年省にメールで確認した（13/01/2012）。

電話の場合、戸口に人がやってきた場合、金融サービスの場合、何かに当選したなど通知の場合、それぞれ疑いを抱くべきサイン・ポイントを紹介している。

6. 自分を守るには何ができるのか？
   犯罪に関する知識や情報をしっかりと持つことの重要性を強調している。相手の良い印象にだまされるな、優しく接することにとらわれるな、などの行動面での助言の他、オレオレ詐欺は電話帳で古めかしいファーストネームを探して狙うので、掲載はイニシャルのみにすべきであるといった具体的なものもある。戸口に人がやってきたばあい、公共の場での犯罪被害の防止ヒント、悪徳商法、オンライン取引など、ケース別に対策が紹介されている。全 13 ページ。
7. 何か起こったら？
   クレジットカードを止めたり、警察への通報を迅速に行うなど指示を挙げている。また、高齢者によく見られる事象として、被害に遭ったことを認めたがらなかったり、自分の不注意により犯罪を招いた事を、子供、親族や周囲の人がどんな目でみるだろうかと考え悩む気持ちが、犯人の検挙を遠のけると指摘している。
8. 高齢者の家族または親族として何ができるか？
   被害を未然に防ぐために家族としてできること、被害に遭ってしまった場合の対処法を推奨している。
9. さらなる情報をどこで得るか？
   警察、消費者団体、市民団体など、情報提供を行っている組織を紹介している。各機関の概要とウェブサイト、電話番号が掲載されている。

図 3.4.1：“Rate mal, wer dran ist? So schützen Sie sich vor Betrügern Trickdieben”より抜粋

Seite 13 Kapitel III Inhalt zurück weiter

Strafanzeige ist eine Tat für den Täter oder die Täterin aber in aller Regel völlig gefahr- und folgenlos.

Auch wenn die betroffene ältere Person Strafanzeige erstattet, rechnen sich manche Kriminelle besonders gute Chancen aus, ohne Strafe davonzukommen. Sie gehen davon aus, dass viele Ältere eher schlecht sehen, sich vielleicht auch nicht mehr in allen Einzelheiten an das Geschehene erinnern und damit vergleichsweise ungefährliche Zeugen sind.

冊子全体を通じて、文字が大きく、高齢者でも読みやすいように配慮がされている。また、文脈に合わせて高齢者をモデルとした写真が挿入されている（図 3.4.1）。
冊子出版後に立ち上げられた、高齢者を犯罪から守るための行動計画「高齢者の安全な生活」"Sicher leben im Alter" (SiliA)の情報誌としても利用されている。[48]

[48] 「定年後の安全な生活－高齢者を支える行動計画」, 29/07/2011
http://www.bmfsfj.de/BMFSFJ/aeltere-menschen,did=173980.html（15/12/2011）

5.　スウェーデン

5.1.　サーフカーム（平穏なネットサーフィン）SurfaLugnt.se

①目的・対象

サーフカームは 2005 年より運営されているネットワーク団体で、スウェーデン政府（健康省 The Ministry of Health、郵政通信庁Post and Telecom Agency）、政府関係団体（Save the Children他）、ITビジネス関係（シマンテック、マイクロソフト他）及び非営利団体により共同運営されている。インターネット上でウィルスの拡散を防ぎ、スパムを取り除き、詐欺行為企図（フィッシング）を検知するなど、スウェーデンにおけるネットサーファーのオンラインでの安全を推進している。[49]

サーフカームでは政府の支援を受け、子供や若者のインターネット利用状況に関する親、大人たちの認識の向上という国家的な取り組みに従事している。スウェーデンでは若い少女の 40%がブログを書き、うち多くは 16 歳から 20 歳の少女たちである。[50]このように若年層のインターネット利用率の高いスウェーデンにおいて、オンラインでのコミュニケーションや情報共有が若者にもたらす利点を肯定しつつも、オンラインでのいじめや個人情報の取り扱いなど、落とし穴となりうる要素を大人たちに認識させることを狙いとしている。

このような目的の一環として、サーフカームのウェブサイト上では、大人や教育者を対象とし、子供や若者のインターネット利用の安全性を確保するためのツールを提供している。チェックリストの代わりに、子供や若者のインターネット利用に関するクイズ（11 問）[51]の他、子供や若者のインターネット上での行動に、親や大人たちが肯定的に（あれこれ禁止するのではなく）介入していくための 8 つの助言[52]が提供されており、これは子供の行動に責任を持つ親や大人の行動チェックリストとしての役割を果たす。

②提供方法

サーフカームのウェブサイト上で無料で提供されている。クイズはスウェーデン語のみ、助言は 12 ヶ国語で用意されている。

「行動計画－高齢における安全な生活 (SiliA)」, 21/07/2011　http://www.bmfsfj.de/BMFSFJ/aeltere-menschen,did=140394.html（15/12/2011）

[49] http://www.pts.se/sv/Internet/Internetsakerhet/For-hemmet/
「 サーフカーム―平穏なネットサーフィンするには脅威を知ろう」Surfa lugnt: Lär känna hoten så surfar du lugnare
<http://www.pro.se/Teknikhornan/Surfa-lugnt/> (14/12/2011)
[50] http://surfalugnt.se/wp-content/uploads/Unga_tjejer_dominerar.pdf (07/01/2012)
[51] http://surfalugnt.se/quiz/(07/01/2012)
[52] http://surfalugnt.se/wp-content/uploads/pdf/engelska.pdf（英語版）(07/01/2012)

③様式・内容

クイズの質問と選択肢を以下に抜粋する。実際のクイズ画面を図 4.1.1 に示す。

Q. ブログを始めるには何歳以上である必要があるか？
11 歳
15 歳
制限はない

Q. 若者が最も信頼できる情報源と考えているのはどれか？
教師
国の百科事典(Nationalencyklopedin)
Google

Q. 若者が風俗サイトに遭遇する割合は？
40%
23%
32%

Q. オンライン上で不適切または不快・攻撃的な写真を見つけた場合はどうするべきか？
何もしない
警察に通報する
ウェブサイトの管理人に通報する

Q. ハッシュタグとは何か？
ドラッグの一種
ウェブの分類の一つ
オンライン上でできること

Q. 若者の重要なコミュニケーションチャンネルとは？
電話
IM (instant messaging)
Facebook

Q. 9-14 歳の子供がメディアと接触する時間の中で、インターネットに費やす割合は？
26%
57%
74%

図 4.1.1：クイズの画面

Testa dina kunskaper

Feministisk potential ställs mot osunda ideal:
Unga tjejer dominerar på bloggen.

11 frågor om ungas vardag på nätet.

Hur gammal måste du vara för att starta en blogg?

11 år.
15 år.
Det finns ingen åldersgräns.

Var tycker ungdomar att de hittar den mest trovärdiga informationen?

Lärare.
Nationalencyklopedin.
Google.

Vad betyder internetförkortningen POS?

Point so taken.
Position over seas.
Parent over shoulder.

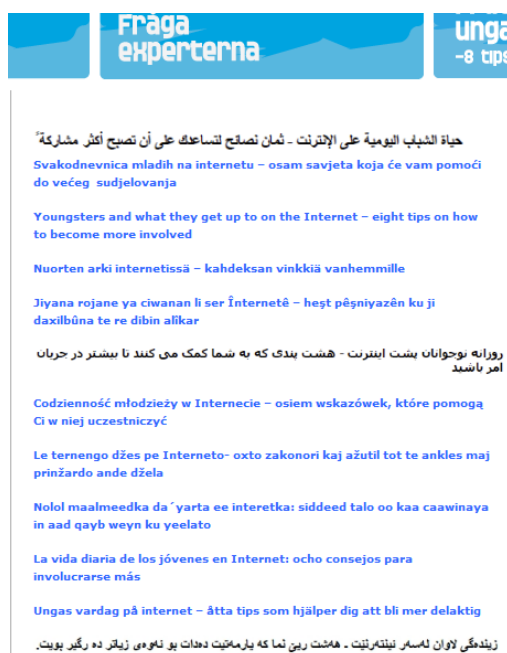
Populära ungdomssajter på nätet

Här nedan har vi listat några av alla de populära sajter där barn och unga hänger på nätet. Gemensamt för de flesta är att de fungerar som sociala mötesplatser där man håller kontakt med befintliga kompisar och lär känna nya.

www.blogg.se
www.bloglovin.com
www.dayviews.com
www.facebook.com
www.flashback.org
www.habbo.se
www.hamsterpaj.net
www.kamrat.com
www.kpwebben.se
www.ls8.se
se.msn.com
www.myspace.com
www.snuttis.se
www.stallet.se
www.tumblr.com
www.twitter.com
www.worldofwarcraft.com
www.wordpress.org
www.youtube.com

中央部分がクイズで、3 択式の問題が 11 問出題される。全て回答すると、正解した問題数と全ての問題に関する解説が表示される。左側のイラストをクリックすると、「若い女の子がブログを支配する」という表題のレポートが開く。クイズのページの右側には、子供や若者に人気のウェブサイトのリンクが紹介されている。

メニューバーの Råd & tips (ヒント)の項目には、子供や若者のインターネット上での行動に、親や大人が良い意味で介入していくための 8 つの助言が、スウェーデン語の他、12 の外国語で紹介されている（図 4.1.2）。これは、親をはじめ子供の世話をする大人たちのためのチェックリストの役割を果たす。

図 4.1.2：各国語の助言のページへのリンク

同ウェブサイトではこの他、子供や若者のインターネットセキュリティに関する情報や、専門機関へのリンクを提供している。また、子供や若者のコミュニケーションに関連するインターネット上の問題に詳しい専門家への質問を送信することもできる。さらに、自分の子供からウェブ上での活動に関し聞き出しにくい親たちのために、大人からの質問に若者の目線で回答するティーンエイジャーにより構成されるパネルがある。これらウェブサイト上で提供されるサービスはいずれも無料で利用することができる。

5.2.　ヨーテボリ市ITガイドラインーチェックリスト

①目的・対象

ヨーテボリ市は2008年秋、同市の情報財産を安全に保守する目的で、情報セキュリティに関する新たなガイドライン ”Riktlinjer för informationssäkerhet i Göteborgs Stad”を発行した。これに基づき、情報セキュリティの統制を図るための手段として、チェックリストを含む６つの資料を2010年に発行した。[53]チェックリストは、ヨーテボリ市の情報セキュリティガイドラインの定める基準を満たす水準の運用が行われているかを判断するするための役割を担う。[54]

対象はヨーテボリ市政府に属する各組織で、主に内部監査目的で使用される。[55]

②提供方法

「ヨーテボリ市情報セキュリティ・ガイドライン （Ver.1 2008 年）」(Riktlinjer för informationssäkerhet i Göteborgs Stad v.1.0) と対になったチェックリストで、「都市のIT」(IT i Staden)ウェッブページ[56]内の添付文書リストに掲載されており、無料でダウンロードが可能である。希望者には紙媒体での配布も行っている。[57]スウェーデン語のみ。

③様式・内容

チェックリストは、80 点におよぶ質問と IT 用語の定義･概念から構成されている（全 9 頁）。質問は Yes/No をチェックする形式で、コメント欄も設けられている。各項目に含まれる質問事項を以下に抜粋する。

情報資産の管理（7 問）
・全ての情報システムのリストを所持している。
・システムオーナーの情報を所持している。
・各情報システムの目的が明確にされている。
・それぞれの情報システムの果たす責任が明確にされている。少なくとも、情報所有者とシステム所有者が明確である。

人材セキュリティー（3 問）
・各情報システムのユーザーマニュアルが文書化されている。
・ユーザーがデータネットワークに関する法律や規制を理解できるだけの資料が用意されている。

物理面・環境面でのセキュリティ(13 問)
・許可なき訪問者のアクセスは制御されている。

---

[53]http://www5.goteborg.se/prod/Intraservice/Namndhandlingar/SamrumPortal.nsf/4CC390011F20F301C12577C30046B792/$File/53010_TU.pdf?OpenElement (07/01/2012)
[54]http://www5.goteborg.se/prod/Intraservice/Namndhandlingar/SamrumPortal.nsf/01F4AD6BB58555F7C1257808002E44C8/$File/tuinformationssakerhet.pdf?OpenElement (07/01/2012)
[55] ヨーテボリ市政府の情報セキュリティ部門にメールで確認した(09/01/2012)。
[56]http://www.goteborg.se/wps/portal/!ut/p/c5/jctBDoIwEEDRs3CCTqcDjEtKDa0asDYYZGO6MIZEwIXR69sbaP7y5YtRpJb4nu7xNa1LfIhBjMUV873XuFPA_ckA6rJnbVjSBpNfkqtA22AUdAUZcJ6PioNEPOf_3HVTWSoPAEwNgCPdtbb2Epz6cbd2nW_iOffDp8qyL3rXyz8!/dl3/d3/L2dJQSEvUUt3QS9ZQnZ3LzZfMjVLUUIySjMwOFVSRDAyQjdVOEJEODE0OTI!/ (07/01/2012)
[57] ヨーテボリ市政府の情報セキュリティ部門にメールで確認した(09/01/2012)。

・データセンターなどの主要な IT 環境においては、訪問者の履歴が残されている。
・同じく訪問者を容易に特定することができる。
・同じく訪問者は適切な職員により監督されている。

情報通信運用コントロール（15 問）
・各 IT システムの運用、また運用上の責任について文書化されている。
・各 IT システムのさまざまな場面における運用方法（再起動、リカバリー、事故管理など）について文書化されている。
・安全性に関する重要なイベントの履歴が残されている。
・各情報システムごとに重要なイベントを追跡できるようにログが管理されている。

アクセスコントロール (8 問)
・職務上の必要性に基づいた、最小限の情報財産へのアクセスが設定されている。
・IT システムの管轄権限の所有はごく少数の者に限られている。
・アクセス権限の登録、登録解消についてのルールと手順が確立、文書化されている。

IT システムの習得･開発･管理 (15 問)
・情報システムの安全性をモニターする手順が確立されている。
・情報システムの安全性の定期的なモニターと評価を行っている。
・情報システムの管理者を交代する場合の正式な手順が確立されている。
・稼働中の IT システムにソフトウェアを導入する場合の手順が確立されている。
・著作権について契約書に定められている。
・システムに関する文書が最新の状態に保たれるよう、手順が確立されている。
・IT システムの脆弱性または問題点をつきとめ、分析するための手順が確立されている。
・脆弱性、問題点を発見するための分析作業が定期的に行われている。

インシデント管理 (8 問)
・インシデント発生時の、情報システムユーザーの行動の意思決定手順が確立・文書化されている。
・情報システムに発生した事故の報告手順が確率・文書化されている。
・同回復手順が確立・文書化されている。
・同モニター手順が確立・文書化されている。
・同分析手順が確立・文書化されている。

ビジネス計画の継続 (8 問)
・データや情報へのアクセスが絶たれてから、ビジネス運営が機能不全になるまでの時間が正式に定められ、文書化されている。
・ビジネス継続のため、正式に採用された計画が存在し、文書化されている。
・IT システムを含む、ビジネス運営の再開・バックアップ手順が、ビジネス継続計画に含まれている。
・年に一度、ビジネス継続計画がテストされている。

フォローアップ (3 問)
・安全性基準を満たしている。
・情報セキュリティが安全性基準のモニター項目に含まれている。
・安全性基準のモニター結果が、組織の幹部に報告されている。

図 4.2.1：ヨーテボリ市ガイドライン　チェックリスト (抜粋)

CHECKLISTA

RIKTLINJER FÖR INFORMATIONSSÄKERHET I GÖTEBORGS STAD

Version 1.0

Hantering av informationstillgångar

Nr	Fråga	Ja	Nej	Kommentar
1.	Har en förteckning över samtliga informationssystem upprättats			
2.	Finns informationsägare utsedda för verksamhetens information			
3.	Har samtliga informationssystem en utsedd systemägare			
4.	Innehåller förteckningen en ändamålsbeskrivning för respektive informationssystem			
5.	Innehåller förteckningen en beskrivning över tillämpliga regler, lagar, avtalsrättsliga åtaganden etc för respektive informationssystem			
6.	Innehåller förteckningen en beskrivning över ansvarsfördelningen för respektive informationssystem. Som minimum ska informationsägare och systemägare finnas definierade.			
7.	Har informationsklassning genomförts och dokumenterats för respektive informationssystem			

Personalresurser och säkerhet

Nr	Fråga	Ja	Nej	Kommentar
8.	Har kraven som ställs på personer som ska få tillgång till respektive informationssystem definierats			
9.	Finns det en dokumenterad användarinstruktion för respektive informationssystem			
10.	Är användarinstruktionen utformad så att en användares behov av att sätta sig in i detaljer kring gällande lagstiftning/regler för informationssystemet minimeras			

5.3. ACTION (高齢者のニーズを満たすテレマティックス*介入による介護者支援サービス－Assisting Carers using Telematics Interventions to meet Older persons' Needs)

①目的・対象

高齢者と障がい者、その介護家族を支援する目的で、1997年にEUプロジェクトとして開始された。[58]具体的には、脆弱な高齢者に自立のためのノウハウを伝授し孤独を緩和、および介護家族のサポート、介護スタッフの職業満足度の向上と自己啓発の推進、高齢者と介護家族の生活の質の向上を狙いとしている。[59]

組織としてのACTIONは、電話会社Teliaと提携するACTION介護ABと調査会社のREACTIONセンターABの二企業から成り立つ。サービスとしてのACTIONはエビデンス（臨床結果）に基づくサポートサービスで、スウェーデン健康科学省とボロース大学のACTION介護スウェーデンABが共同開発した。

②提供方法

サービスは、テレマティックス（コンピューター機器と移動体通信技術を組み合わせることによって、無線で情報を送受信できるようにする仕組みのこと。ビデオ電話に類似。）を用いて提供される。国内外（例えば上海）の会議やミーティング、高齢者ケアデーなどさまざまな場所でプログラムの紹介を行っている。[60]

③様式・内容

ACTIONサービスはACTIONプログラム、ビデオ電話つきコンピューター、ACTIONコールセンター、教育とサポートの4本柱から成り立つ。

1. **ACTION（マルチメディア）プログラム**は日常生活の介護について、飲食、移動操作、失禁、床擦れ、発作、ライフケアの終焉に至るまで指導する。健康と社会的ケアサービスの意思決定情報を提供し、補助器具または公共サービスガイドの情報提供を促進する。息抜き、エクササイズプログラムも含む。

2. **ACTIONビデオ電話つきコンピューター**はソフトウェアとウェッブカメラをインストールすることによって、高齢者がビデオ電話を通じて遠隔地に居住する子供や孫と連絡を取り合うことも可能となる。

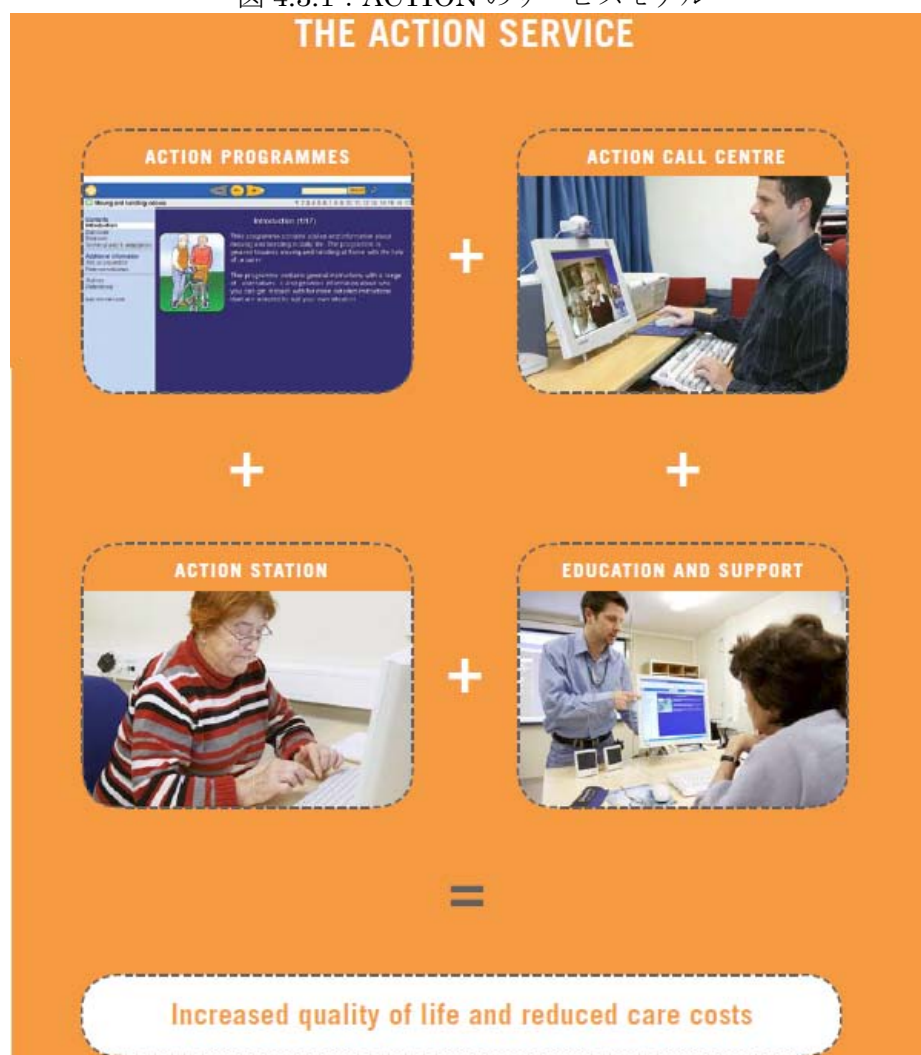
3. **ACTIONコールセンター**では、ACTIONビデオ電話を使って経験豊富な健康管理担当職員がコールセンターにて対応し、高齢者とその介護者をサポートする。ACTIONセンター職員はネットワークの新設を補助し、新しいユーザーへサービスの紹介と訓練を行い、その後はユーザーの状況を継続的にモニタリングする。

4. **教育とサポート**では地方政府がACTIONプログラムを導入するときに実施計画を立て相談に乗る。ACTIONと共同で働く健康・社会的ケア担当職員を教育する。高齢者とその家族とともに、教育説明会のスタッフが使う計画やマニュアル作成をサポートする。コールセンター職員と共同で家庭でブロードバンドや機器のインストールや技術サポートの手伝いをする。

---

[58] http://www.actioncaring.se/Eng/EngActionfolder.pdf p.2 (09/01/2012)
[59] Ibid. p.3 (09/01/2012)
[60] http://www.actioncaring.se/Eng/Engpress.htm (09/01/2012)

5. **痴呆プログラム**として、早期の痴呆症状を発症した高齢者とその家族、世話役のために、以下のような支援を提供している。
   - 情報・教育プログラム（マルチメディアプログラム）には、自身の病気の理解や記憶を助けるための訓練や、他人と接触を持つ社会活動やインターネットの利用などが含まれる。さらに、コンピューターを使った認識訓練も提供している。
   - 12 週間サポートプログラムは、早期痴呆患者とその家族を支援するものである。痴呆患者のケアのプロの指導の下、メンバーは毎週 3 時間顔を合わせ、一緒にマルチメディアプログラムを行い、意見交換を行う。

図 4.3.1：ACTION のサービスモデル

出典：Increased quality of life and independence for older people and their families (英語版)

6.　シンガポール

6.1.　ファースン・アップ（しっかり締めろ）Fasten up!

①目的・対象

シンガポールの Infocomm Security Division (iSec)は、シンガポールにおいて安全な情報コミュニケーションインフラストラクチャーを確立、運営を担う組織で、政府の情報セキュリティ政策やガイドラインの策定を監督している。

Fasten Up! は、コンピューターを安全に運用する上で導入が推奨されるファイアウォール（Firewall）、アンチウイルス（Anti-virus）、悪徳商法（Scam）、アップデート（Update）、パスワード（Password）という 5 種類の重要な IT セキュリティ用語の頭文字を取って名づけられ、これらに関する認識を向上させることを狙いとしたコンテンツで、情報の漏洩を防ぐため「しっかり締めろ」という意味との掛詞となっている。

各用語の説明に織り込まれるアニメや写真から、若者を対象としていると思われる。

②提供方法

Go Safe Online というウェブサイト[61]に掲載されており、無料で閲覧が可能。英語のみ。

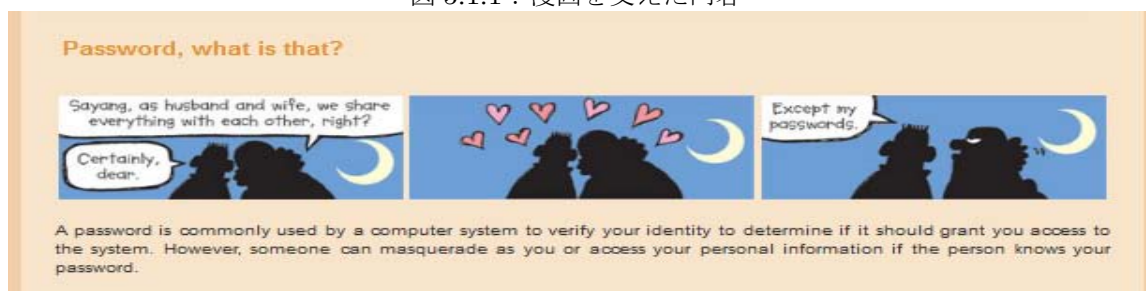
③様式・内容

同ウェブサイトには、以下の 3 種類のツールが存在する。

(1) Fasten Up!

チェックリストは存在しないが、クイズ形式で Fasten Up! の名称の基となる 5 種類の重要用語が解説されている。質問は、それぞれの用語に対し 3 から 9 問で構成されている。用語の説明には 2､3 コマの漫画も含まれており、わかり易くかつ楽しく学べるよう工夫が見られる（図 5.1.1）。

図 5.1.1：漫画を交えた内容

(出典：http://www.singcert.org.sg/awareness/passwords.htm)

各項目に関し、用語の説明、何故それらが必要なのかに加え、関連する便利な情報を提供している。悪徳商法 Scam のページには、ケーススタディとして、電子メールによる Scam、個人情報漏洩による成りすまし詐欺、フィッシングの実例として、新聞記事へのリンクが載せられ

[61] http://www.singcert.org.sg/awareness/index.htm (12/01/2012)

ている。また、アップデートのページには、自分のコンピューターにあるソフトウェアが最新のものであることを確認する方法が、スクリーンショットをまじえて順を追って解説されている(図 5.1.2)。

図 5.1.2：ソフトウェアのアップデートを促す内容のページ

How do I ensure my software is updated?

Update Operating System and Other Software Regularly

The most important piece of software that you should update is your Operating System (OS). For Microsoft Windows users, go to windowsupdate.microsoft.com to check for and obtain updates for your OS. Some software (e.g. Microsoft Windows) has an automatic software update features. Use them to ensure that you always have the latest software patches.

Windows XP with Service Pack 2 comes with a user-friendly configuration screen as shown below, where you can easily turn on the Automatic-Update feature:

Click Start > Control Panel > Security Center
or
Click Start > All Programs > Accessories > System Tools > Security Center

Click image for larger view

For more information on the detailed steps, check out: http://www.theeldergeek.com/security_center.htm

The following screenshots show the process of updating Windows XP Operating System manually. Of course you can choose to do auto-update by enabling the "Auto-Update" feature.

Click image for larger view

(出典：http://www.singcert.org.sg/awareness/updates.htm)

(2) リソース

リソースページも充実している。プレゼンテーションによる IT セキュリティのトレーニングは、以下の 6 モジュールから構成されており、それぞれのモジュールにはアニメーションを駆使したクイズが含まれ、楽しみながら学習することができる。図 5.1.3～5.1.5 に、いくつかのクイズ形式を抜粋し紹介する。

- 導入
- オフィスでの IT セキュリティ
- オフィス外での IT セキュリティ
- 電子メールのセキュリティ
- 安全なブラウジング
- ファイナルチャレンジ

図 5.1.3　導入モジュールの IT セキュリティの認識度評価 20 問のクイズ(Yes/No 二択式)

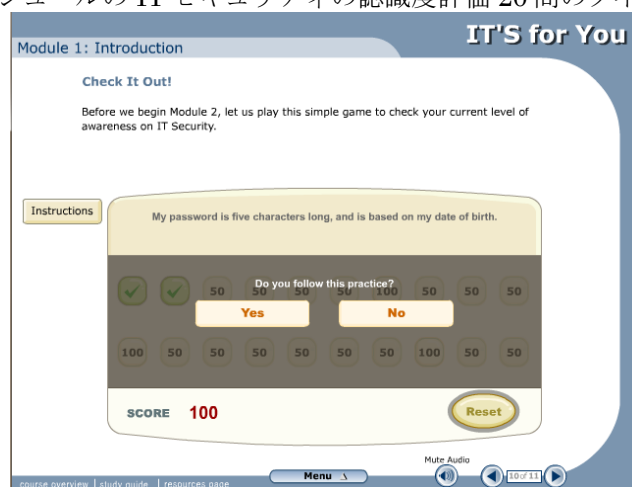



図 5.1.4　オフィス外での IT セキュリティモジュールのクイズ

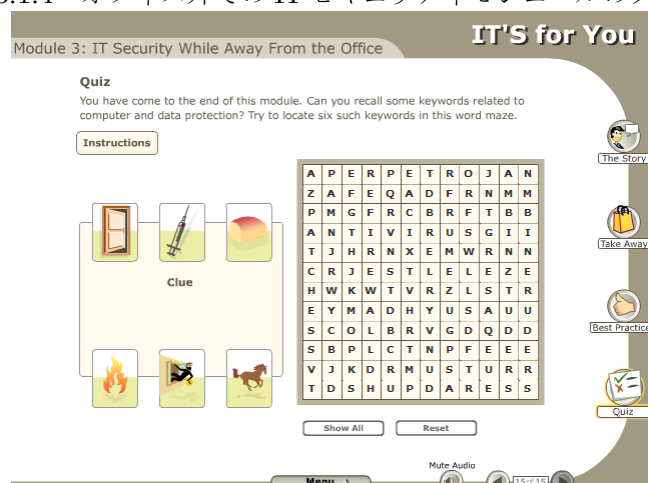
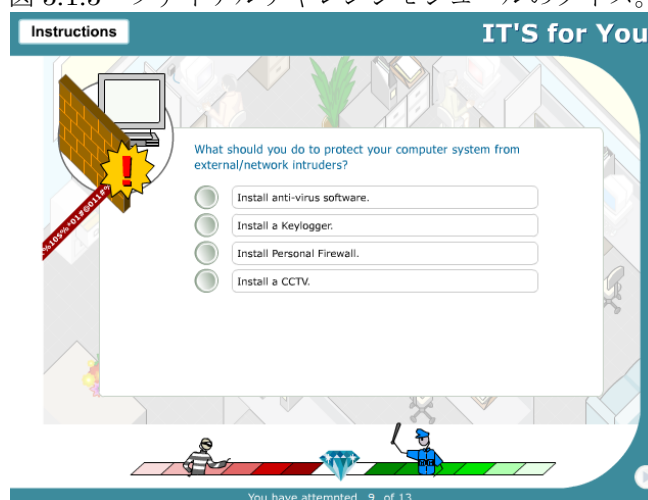



図 5.1.5　ファイナルチャレンジモジュールのクイズ。

一問ごとに正解すると警察が、不正解だと泥棒がダイヤモンドに近寄るアニメーションが挿入されている。

この他、スパイウェア、フィッシング、モデムジャッキングの解説（形式は(1) Fasten Up! の解説に類似）をする情報と助言のページ、ダウンロード可能なセキュリティ・パンフレット（漫画での説明を含む 24 頁、2010 年[62]）、指導者のための訓練ワークショップの案内、5 種類のITセキュリティ用語についてのアニメーションで構成されている。

(3) 情報セキュリティクイズ (Quiz)

クイズのページ（http://www.singcert.org.sg/awareness/quiz.htm）では、正誤クイズ(10 問)で情報セキュリティの意識向上を図っている。

クイズは一問ごとに True または False をクリックすると、その場で正解と解説が現れる。アンチウィルスソフト、ファイアウォール、悪徳商法への対応、パスワード設定等に関する基本的な問題を扱っている。

図 5.1.3: クイズの画面

(出典：http://www.singcert.org.sg/awareness/quiz2.htm)

また、スパイウェアコンテスト（3 問）に正解を送った最初の 50 人にはショッピング割引券が送られるプロモーションも行われている。[63]

---

[62] パンフレット: <http://www.singcert.org.sg/awareness/security.htm> (10/01/2012)

[63] 「スパイウェアコンテスト」 <http://www.singcert.org.sg/awareness/spyware_contestr.htm> (14/12/2011)

6.2. サイバロニア：バーチャルサイバーセキュリティ・パーク　Cyberonia: Virtual Cyber Security Park

①目的

サイバーセキュリティ意識啓発連合 (Cyber Security Awareness Alliance) とシンガポール犯罪防止局(National Crime Prevention Council) は、小学生の間で情報セキュリティ保守のための正しい認識を普及させるため、Virtual Cyber Security Parkを開発した。[64]同プログラムは、シンガポールセキュリティマスタープラン 2 (MP2: Infocomm Security Masterplan 2) 事業のうちのひとつで [65]、2011 年 4 月 8 日より導入された。この背景には、2008 年の研究で、若年層のコンピューターの利用が高まる中、彼らのオンライン上での安全性や責任に関する認識が非常に低いことが判明した事実がある。[66]

対象となるのはシンガポールの小学生 5 年生の全児童で[67]、インタラクティブな コンピューターゲームを通じて健全で安全なサイバー利用法を学ぶことができる。ゲームは確実に子供たちが十分楽しめるようにデザインされている。[68]

②提供方法

ウェブサイト（http://cyberonia.org.sg/ncpc/index.php/ncpc/register）で利用登録を行う。小学校の名前も選択しなくてはならない。同じサイトからアクセスが可能である。

犯罪防止局はウェブ等の媒体を使って積極的に同ゲームの普及に努めている。また、シンガポールの小学校のウェブサイトで紹介されている例もある。[69]

③様式・内容

3Dテクノロジーを使い、子供たちがオンライン中に遭遇するシナリオとしてソーシャルネットワークのプロフィールを作成したり、オンラインゲームで遊んだりする状況を再現する。[70]
ゲームのコンセプトはカウンセラー、サイバー認識を教える教師、ゲーム擁護者、警察関係者、法律家、他分野の専門家と相談の上で開発された。[71]ゲームに参加することによって、児童たちは以下のような内容を学ぶことになる。

- オンラインでの安全性
- 法律遵守

---

[64] http://app.mica.gov.sg/Default.aspx?tabid=36&ctl=Details&mid=539&ItemID=1126 (08/01/2012)
[65] "Singapore Tries Virtual Cybersecurity Park", *thenewnewinternet.com*, http://www.thenewnewinternet.com/2010/03/22/singapore-tries-virtual-cyber-security-park/ (15/12/2011)
[66] "National Crime Prevention Council Annual Report 2010/2011": p.6 <http://www.ncpc.gov.sg/pdf/annual2011.pdf> (08/01/2012)
http://cyberonia.org.sg/ncpc/index.php/ncpc/parents (08/01/2012)
[67] http://cyberonia.org.sg/ncpc/index.php/ncpc/parents (08/01/2012)
[68] "Singapore Tries Virtual Cybersecurity Park", *thenewnewinternet.com*, http://www.thenewnewinternet.com/2010/03/22/singapore-tries-virtual-cyber-security-park/ (15/12/2011)
[69] http://www.aitong.moe.edu.sg/cos/o.x?c=/wbn/pagetree&func=view&rid=1124502
[70] Chua Hian Hou, "A 'park' to teach kids cyber safety", *AsiaOne Education,* available at http://www.asiaone.com/News/Education/Story/A1Story20100324-206453.html (15/12/2011)
[71] "Factsheet on Cyber Security Awareness Alliance", issued on 9/2/2011, pp.2-3. http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20070402172309/Factsheet_CSAA.pdf (08/01/2012)

- ゲーム中毒
- 望ましくないコンテンツの対処法
- 自身の安全性を保守しつつ健全なコンピューター利用をする方法

ゲームコンセプトのうちいくつかは、児童にバーチャル都市の土地を割り当て、何かを生産させるよう任務を与えるものもある。ヴァーチャル都市の中でプレーヤーは自分を象徴するアバターを創る。プレーヤーは自分なりの都市を建造する際、個人としてもグループとしても参加することができる。建設プロセスを通じて、児童はある程度の挑戦に遭遇したり、ミニゲームに参加したりするが、それらによって特別なサイバーセキュリティ技能に関する知識や経験を得られるよう構成されている。[72]

同ゲームの利用は無料であり、児童たちは各自のペースでゲームを通じて学習を進めることができる。また、教員が同伴して逐一指示を出す必要もなく、各家庭で利用可能。ゲームは開始から 2 週間開放され、朝 7 時から夜 10 時まで利用できる。ただし、利用可能な時間は一日に 2 時間だけで、合計 10 時間以内にゲームを終了しなくてはならない。[73]

図 5.2.1：導入のページ

図 5.2.2：サイバーセキュリティに関するページ

[72] "Factsheet on Cyber Security Awareness Alliance", issued on 9/2/2011, pp.2-3.
http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20070402172309/Factsheet_CSAA.pdf (08/01/2012)

[73] http://cyberonia.org.sg/ncpc/index.php/ncpc/parents (08/01/2012)

6.3. シルバー・インフォコム　Silver Inforcomm Initiative (SII)

①目的・対象

Silver Inforcomm Initiative (SII) は、シンガポールIT開発局 (IDA Singapore (IDA: Infocomm Development Authority of Singapore)) が提供する 50 歳以上の 高齢市民を対象とした取り組みで、学歴、言語、IT 能力の違いに対応しながら情報技術格差 (デジタルデバイド) の橋渡しをすることを目的としている。高齢市民はデジタルライフスタイル技術の訓練を受け、デジタル時代の利便性を享受することができるようになる。

②提供方法

同プロジェクトにはにはいくつかの異なるプログラムが含まれるが、いずれも参加型の講義形式で、市民が直接コンピューターに触れながら使い方を習得する。以下に代表的なプログラムの詳細を記載する。

IDAでは、セミナーや展示会など国内各地でのイベントを通じ、SIIの取り組みの普及に努めている。[74]テレビでの宣伝は行っていないが、イベントやワークショップのビデオを紹介するビデオを作製し、You Tube のIDAのチャンネルに掲載している。[75]また、Facebook、Twitter、Flickrやニュースレターなど、さまざまな媒体を用いて、SIIを含む各種取り組みを紹介し、普及活動を行っている。

③様式・内容

- Silver Infocomm Junctions (SIJ)
2007 年より開始。[76]高齢者にやさしく便利な立地のIT習得拠点が、国内に 9 箇所設けられている。政府はさらに高齢者へのIT利用の普及を加速させるため、2011 年に新たにSIJ 3 箇所の設置を決定し、総数 12 箇所になる予定である。[77]トレーニングは一時間あたり 5～10 シンガポールドル程度の良心的な価格で提供されている。[78]

- Silver Infocomm Curriculum
SIJで開催されるコースにはコンピューター・インターネット基礎、インターネット取引、ITセキュリティ、インターネット・バンキングなどを含むシニア用 12 テーマがあり、初心者向けのiBEGIN、中級者向けのiLIVEというプログラムにより編成されている。iBEGINではコンピューターの基本操作方法、オンラインで自身を保守するためのセキュリティ情報、ビデオ電

---

[74] IDA Singapore にメールで確認した (11/01/2012)。

1. [75] http://www.youtube.com/idasingapore (07/01/2012)

[76] http://www.asiaone.com/News/AsiaOne+News/Singapore/Story/A1Story20100920-238061.html (07/01/2012)

[77] "More than 6,000 attend SID 2011", Infocomm News From Singapore iNSG, 28/09/2011 (07/01/2012)
http://www.ida.gov.sg/insg/post/More-than-6000-attend-SID-2011.aspx (16/12/2011)

[78] http://www.ida.gov.sg/Programmes/20060419135418.aspx?getPagetype=34 ただし、一時間 2～6 シンガポールドルと記載する情報源もある。（"Two Silver Infocomm Junctions (SIJ) Opened for Senior Citizens", sgcGo.com, http://sgcgo.com/silver-infocomm-junctions/ (19/12/2011)）

話やインターネットの使い方、iLIVEではオンライン決済や写真の編集方法なども含まれる。教材は英語と中国語で用意されている。[79](ダウンロード可能な資料などは見当たらない)

- Silver Infocomm Hotspots

高齢市民に無料でコンピューターとインターネットサービスへのアクセス提供する施設で、コミュニティーセンターや高齢者関係エリア、民族や宗教ごとの集会所など、利用者にとって身近な場所に開設されている。2011 年 3 月の時点で全国に 34 箇所設置されていたが、2012 年末までに 100 箇所まで増設が計画されている。[80] Silver Infocomm Hotspotsでのコンピューター利用は無料である。

- Silver Infocomm Day

IDAとIT産業、コミュニティの共同で毎年開かれる高齢市民のためのイベント。[81]トーク、展示会、実践訓練の 3 つが一度に楽しめるイベントで、2007 年の開始以来のべ 4,500 人が参加した。2011 年 9 月 17 日から 19 日の間に 南洋理工学院（Nanyang Polytechnic）で開かれたSilver Infocomm Dayには 2,000 人を超える参加者があり、その後の他 2 会場での開催分を含めると、合計約 6,000 人の参加者が見込まれる。[82] Silver Infocomm Dayでは無料のITセミナー、一回の参加費 10 シンガポールドルのワークショップ、スポンサーから提供されるコンピューターや携帯電話が当たる抽選会が開かれ、高齢の参加者を引き付ける方法をとっている。[83]

- Inter-generational IT Bootcamps

国内の学校と共同で開催するITワークショップで、2010 年より開始された。コンピューター利用技術の習得と共に、学生とその祖父母との間の世代を超えた交流の促すことを目的としている。[84]コンピューター教室へ通うのとは異なり、自分の孫と一緒に学べるという環境が付加価値を生み出す。情報検索や電子メール、Facebookの使い方などの他、手書き認識タブレットを使った中国語の入力、オンライン健康ツールを使用するなど、高齢者に特化した内容が含まれている。[85]参加者とその孫には、コース修了書も授与される。[86]尚、参加費は無料である。[87]

---

[79] http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20060530162222/Factsheet-SII.pdf (07/01/2012)

[80] "Silver Infocomm Initiative", iDA Singapore. http://www.ida.gov.sg/Programmes/20060419135418.aspx?getPagetype=34 (16/12/2011)

[81] "Silver Infocomm Day, 28-29 November 2009, Singapore Polytechnic" の様子を以下のリンク先から見ることができる。http://www.youtube.com/watch?v=eL3OLJxeKOU&NR=1&feature=endscreen (10/01/2012)

[82] "More than 6,000 attend SID 2011". (16/12/2011)

[83] "September 2010 Media Factsheet, Silver Infocomm Initiative", iDA Singapore, 2010. http://www.egov.gov.sg/c/document_library/get_file?uuid=a031688d-bf9f-4726-bb92-1b6a8c7f6b91&groupId=10157 (19/12/2011)

[84] "August 2011 Factsheet: Silver Infocomm Initiative", iDA Singapore, 2011. http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20060530162222/Factsheet-SII.pdf, p.4 (10/01/2012)

[85] http://www.ida.gov.sg/insg/post/SII-New-Silver-Infocomm-Junction-opens-in-Tampines.aspx (10/01/2012)

[86] Inter-Generational IT Bootcamp http://www.youtube.com/watch?v=qFiaWUQHFU0 (10/01/2012)

[87] IDS Singapore にメールで確認した (11/1/2012)。